ANL/NSE-18/13

# Improvements and Path Forward for Regulatory Acceptance of SAS4A/SASSYS-1

**Nuclear Science and Engineering Division**

ANL/NSE-18/13

# Improvements and Path Forward for Regulatory Acceptance of SAS4A/SASSYS-1

**prepared by**
**Acacia J. Brunett, Lander Ibarra, Thomas H. Fanning, and Rui Hu**
Nuclear Science and Engineering Division, Argonne National Laboratory

October 31, 2018

# EXECUTIVE SUMMARY

In the U.S., a key component of the commercialization of advanced reactors is completion of a license application, which must ultimately be approved by the Nuclear Regulatory Commission (NRC). The NRC's approval of the license application is contingent on, among other things, satisfactory demonstration of the design basis and response to transient and accident scenarios using accepted codes and methods. This effort seeks to improve the regulatory acceptability of the SAS4A/SASSYS-1 advanced reactor design and safety analysis system software by identifying and addressing gaps in the SAS4A/SASSYS-1 documentation basis that support software qualification and dedication. The software's unique capabilities to assess inherent fast spectrum feedback effects and passive safety features, which facilitate assessment of key safety metrics, position it as a key licensing tool in the field of sodium-cooled fast reactors (SFR).

Like most legacy software that has primarily existed in the R&D space, the most significant challenge facing SAS4A/SASSYS-1 for use in a licensing framework is the availability of a documentation basis that describes the code's pedigree. While the code has been used for licensing of FFTF and the design of the CRBR Plant, the historical verification and validation (V&V) activities supporting SAS4A/SASSYS-1 development largely do not align with the modern software quality assurance (SQA) and V&V requirements that exist today.

To that end, two approaches for use of SAS4A/SASSYS-1 in a commercial licensing framework have been targeted for this effort: commercial-grade dedication (CGD) and software qualification. Given the broad range of regulatory guidance and requirements on these topics, for the purpose of this report the methods and requirements prescribed in the ASME NQA-1-2008/2009 Standard and Regulatory Guide 1.203 on the evaluation model development and assessment process (EMDAP) have been utilized to develop a qualification and dedication requirements matrix centered on the following fundamental software verification and validation activities and requirements:

- Verification: software requirements specification, software design description, acceptance testing
- Validation: analytical benchmarks, separate effects tests, integral effects tests, standard nodalization tests

A key element of software qualification and dedication includes determination of software acceptance with respect to key critical characteristics relevant to the functional requirements of the software (e.g. the software's ability to model specific phenomena for a well-defined set of transients and model input). To assist with identification of cross-cutting transient phenomena and functional requirements, domestic SFR vendor designs have been reviewed to identify a reference SFR design. For the purpose of this report, the reference design is defined as a pool-type reactor with metal alloy fuel, a liquid-metal intermediate heat transport system, and passive decay heat rejection systems. Given this reference design, a series of high-level cross-cutting phenomena was identified for a general class of single-fault undercooling or reactivity insertion transients that scopes the design basis space, with the goal of assisting with prioritization of documentation development efforts for key transient models in SAS4A/SASSYS-1:

- Reactivity feedback response prior to scram
- System-wide thermal inertia
- Transition in natural circulation flow regime in heat removal systems
- Decay heat generation
- Steady-state fuel characterization
- Clad/fuel behavior at elevated temperatures

- Point kinetics and decay heat
- Pump coastdown behavior
- Core flow redistribution in loss of forced convection
- Pool stratification

To improve the regulatory acceptability of the SAS4A/SASSYS-1 advanced reactor safety analysis system software, a software qualification and dedication gap analysis as it relates to code documentation has been performed. This effort leverages the expertise and framework established as part of the SAS4A/SASSYS-1 SQA Program. The outcome of this effort is the prioritized list of gaps defined below. These areas should be addressed on a prioritized basis for the cross-cutting phenomenological models identified for their relevance to functional requirements and critical characteristics.

**SAS4A/SASSYS-1 Software Qualification Priorities**

| Gap | Importance | Lead Time | Comment |
|---|---|---|---|
| *Valid Numerical Model Bounds* | High | Medium | Can be completed for high-priority models in short term, but comprehensive documentation requires medium lead time. |
| *Valid Input Bounds* | High | Medium | Can be completed for high-priority models in short term, but comprehensive documentation requires medium lead time. |
| *Software Design Description per component* | High | Medium | Code Manual provides fairly comprehensive design description, however limited documentation of model applicability and input limitations is available. |
| *Validation Matrices* | Medium | Short | Additional review of existing test problems is required to characterize relevant detailed phenomena. |
| *Verification Testing per component* | Medium | Medium | Partially addressed by existing V&V Test Suite. Needs to be resolved on case-by-case basis. |
| *Software Requirements Specification per component* | Medium | Long | Limited requirements documentation available. |
| *SET/IET Validation* | Medium | Long | Should be completed on prioritized basis as per findings of mature validation matrices and review in Section 3.2. |
| *Sensitivity Analysis/ Uncertainty Quantification* | Medium | Long | Supports identification of inherent numerical errors. Requires very long lead time for comprehensive, effective studies. |
| *V&V Test Suite* | Medium | Ongoing | Test suite improvement expected to occur throughout lifetime of project. |
| *Default/Suggested Inputs* | Low | Medium | Can be completed in part in conjunction with identification of valid input bounds. |

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# ACRONYMS

| | |
|---|---|
| ARC | Advanced Reactor Concepts, L.L.C. |
| ASME | American Society of Mechanical Engineers |
| CFD | Computational Fluid Dynamics |
| CGD | Commercial-Grade Dedication |
| CI | Configuration Item |
| CMP | Configuration Management Plan |
| CNWG | Civil Nuclear Working Group |
| CRBR | Clinch River Breeder Reactor |
| CRP | Coordinated Research Project |
| CS | Coding Standard |
| DOE | Department Of Energy |
| DRACS | Direct Reactor Auxiliary Cooling System |
| EM | Evaluation Model |
| EMDAP | Evaluation Model Development and Assessment Process |
| EPRI | Electric Power Research Institute |
| FFTF | Fast Flux Test Facility |
| FMEA | Failure Modes and Effects Analysis |
| FOA | Funding Opportunity Announcement |
| FOM | Figure Of Merit |
| GEM | Gas Expansion Modules |
| IAEA | International Atomic Energy Agency |
| IEC | International Electrotechnical Commission |
| IET | Integral Effect Test |
| IHTS | Intermediate Heat Transport System |
| IHX | Intermediate Heat Exchanger |
| INERI | International Nuclear Energy Research Initiative |
| ISO | International Organization for Standardization |
| LOF | Loss Of Flow |
| LOFWOS | Loss Of Flow WithOut Scram |
| LWR | Light Water Reactor |
| NC | Natural Circulation |
| NQA | Nuclear Quality Assurance |
| NRC | Nuclear Regulatory Commission |
| PIRT | Phenomena Identification and Ranking Table |
| PRA | Probabilistic Risk Assessment |
| PRISM | Power Reactor Innovative Small Module |
| QA | Quality Assurance |
| RG | Regulatory Guide |

| | |
|---|---|
| RVACS | Reactor Vessel Auxiliary Cooling System |
| SDD | Software Design Description |
| SE | Software Engineering |
| SESAME | Safety Assessment of Metal Cooled Reactors |
| SET | Separate Effect Test |
| SFR | Sodium-cooled Fast Reactor |
| SHRT | Shutdown Heat Removal Tests |
| SQA | Software Quality Assurance |
| SQAP | Software Quality Assurance Plan |
| SRP | Software Review Plan |
| SRS | Software Requirements Specification |
| STP | Software Test Plan |
| TOP | Transient OverPower |
| TR | Technical Report |
| TREAT | Transient Reactor Test Facility |
| TUC | Transient UnderCooling |
| TWR | Traveling Wave Reactor |
| UQ | Uncertainty Quantification |
| V&V | Verification and Validation |

# 1 Introduction

In the U.S., a key component of the commercialization of advanced reactors is completion of a license application, which must ultimately be approved by the Nuclear Regulatory Commission (NRC). The NRC's approval of the license application is contingent on, among other things, satisfactory demonstration of the design basis and response to transient and accident scenarios using accepted codes and methods. This effort seeks to improve the regulatory acceptability of the SAS4A/SASSYS-1 [1] advanced reactor safety analysis system software by identifying and addressing gaps in the SAS4A/SASSYS-1 documentation basis that support software qualification and dedication.

The SAS4A/SASSYS-1 design and safety analysis code, developed and maintained by Argonne National Laboratory, provides the transient simulation of anticipated operational occurrences, design basis accidents, and design extension conditions in liquid-metal cooled fast reactors. The code maintains unique capabilities to account for inherent fast spectrum feedback effects and passive safety features, key elements of the sodium-cooled fast reactor (SFR) safety basis. The software facilitates assessment of key safety basis metrics, including margins for structural thermal limits, metallic fuel failure, sodium boiling, and fission product release.

Like most legacy software that has primarily existed in the R&D space, the most significant challenge facing SAS4A/SASSYS-1 for use in a licensing framework is the availability of a documentation basis that describes the code's pedigree. While the code has been used for licensing of the Fast Flux Test Facility (FFTF) and was expected to be used in licensing of the Clinch River Breeder Reactor (CRBR) Plant, the historical verification and validation (V&V) activities supporting SAS4A/SASSYS-1 development largely do not align with the modern software quality assurance (SQA) and V&V requirements that exist today. Furthermore, SQA and V&V requirement evolution in the last twenty years has outpaced fast reactor analysis capability pedigree support due to resource limitations.

Two avenues for use of SAS4A/SASSYS-1 in a commercial licensing framework have been identified for this effort: commercial-grade dedication (CGD) and qualification. While the definition of each can vary per standard or guidance document, for the purpose of this report, CGD shall refer to the formal process prescribed by the ASME NQA-1-2008/2009 Standard [2, 3], while software qualification shall refer to any regulatory-acceptable process for determining acceptance of an evaluation model (EM). With the aim of meeting the broadest spectrum of qualification requirements that exist domestically, Regulatory Guide 1.203 on the evaluation model development and assessment process (EMDAP) will be utilized to identify software qualification requirements for SAS4A/SASSYS-1. Both the NQA-1 Standard and RG 1.203 are industry-recognized methods for determining and documenting software acceptance. As part of this effort, these standards and requirements are reviewed and qualification and dedication requirements matrices have been developed, the results of which are provided in Section 2.

A key element of software qualification and dedication includes determination of software acceptance with respect to key critical characteristics. These critical characteristics define the features, capabilities, and attributes a software must be able to demonstrate with some level of confidence over a prescribed range or operating envelope. For the purposes of a licensing safety analysis, critical characteristics by which a software will be measured will primarily relate to the software's ability to model specific phenomena for a well-defined set of transients. To that end, domestic SFR vendor designs have been reviewed to identify a common set of plant features. These plant features are then utilized to identify a set of generic transients and cross-cutting phenomena. Given this listing of cross-cutting phenomena, the documentation basis for SAS4A/SASSYS-1 can then be evaluated for its ability to support qualification and dedication requirements. The evaluation of SFR design features and event sequences completed as part of this work is provided in Section 3, with the qualification and dedication gap assessment for SAS4A/SASSYS-1 provided in Section 5.

The remainder of this document is structured as follows. Section 2 provides background on the relevant software dedication and qualification requirements a domestic vendor or utility are expected to utilize in the safety analyses contained within a license application. An overview of SFR design features, event sequences, and related phenomena is provided in Section 3. The status of software qualification-related activities for SAS4A/SASSYS-1 is outlined in Section 4. Section 5 entails a gap analysis regarding the documentation required to support use of SAS4A/SASSYS-1 in a license application. Lastly, the conclusions of this effort and a path forward are identified in Section 6.

# 2 Qualification and Dedication Requirements

This section outlines the software qualification and commercial grade dedication requirements a commercial applicant is expected to utilize during a safety analysis contained within a license application. Completion of safety analyses in support of a license application or authorization requires the applicant to demonstrate appropriate usage and application of an analysis software with an acceptable pedigree. In most cases, the applicant will pursue a qualification or software dedication process which demonstrates and documents the acceptability of the software for the specified application. Acceptance of the code during qualification/dedication typically includes review of both the verification and validation properties of the software.

In general, use of any nationally-recognized standard is acceptable provided sufficient justification for applicability of that standard is made. While there is a myriad of standards and requirements documents an applicant may potentially utilize in this process, the most prevalent requirements, Regulatory Guide 1.203, on the evaluation model development and assessment process (EMDAP) (Section 2.1), and NQA-1-2008/2009 (Section 2.2) are described here as these are expected to be the most relevant and rigorous requirements. An overview of EPRI Technical Report 3002002289 on acceptance of commercial-grade design and analysis software use in safety-related applications, a methodology which has previously been utilized by industry in commercial licensing in compliance with the NQA-1 standard, is provided in Section 2.3. A summary matrix outlining the qualification and dedication requirements is provided in Section 2.4.

## *2.1 Regulatory Guide 1.203*

Regulatory Guide 1.203, "Transient and Accident Analysis Method," [4] was developed by the U.S. NRC to provide guidance in development and assessment of the evaluation models (EMs) utilized in accident and transient analyses in a license application. In RG 1.203, an evaluation model (EM) is defined as "the calculational framework for evaluating the behavior of the reactor system during a postulated transient or design-basis accident" [4], meaning an EM may include multiple computer programs as well as all information needed to apply the calculational framework to a specific event. When developing, assessing, and reviewing the EM, it is important to consider the entire framework. That is, the EM is specific to a plant (model) and accident scenario and includes the software and its constituent phenomenological models as well as user input used to describe the plant and transient scenario.

This document also delineates the EMDAP which should be used in determination of adequacy of an EM. Note that EMDAP is *not* applied to a software in the interest of qualifying it for *all possible plant configurations and transients*, but instead is applied to the software and its associated inputs that are being used to model a specific plant configuration and transient.

The EMDAP contains four primary elements regarding EM development and assessment. These elements and associated background for each element are described briefly in Table 2.1, with additional details on the elements below. It should be noted that RG 1.203 targets LWR phenomena, and therefore many of the examples provided by the document are only relevant to LWR transients.

The EMDAP also requires usage of an appropriate SQA standard and development of supporting documentation for the EM development and assessment elements in Table 2.1. Documentation should be maintained current to facilitate efficient reviews. It is important to note that the complexity of the problem will dictate the level of detail and rigor required for EM development and assessment. For relatively simple events, many steps may need to be addressed only briefly, whereas more complicated scenarios and/or EMs may require more robust evaluation. Additional details on SQA best practices and documentation requirements cited by RG 1.203 are provided at the end of this subsection.

Element 1 of the EMDAP involves the establishment of the requirements for the EM, including the scope of application, relevant phenomena and processes, and key parameters. The first step involves defining the analysis purpose as the ultimate purpose of the analysis may affect the relevant figures of merit, assessment base, or acceptance criteria. Step 2 includes specification of figures of merit (FOM) for the analysis. These FOM are typically directly correlated with associated regulations. A typical LWR example includes the margin to departure from nucleate boiling. In Step 3, the basic characteristics of the EM are defined. A hierarchical example of EM characteristics includes: the system and its subsystems (e.g. primary, secondary, containment, etc.); modules (reactor vessel, steam generator, piping, etc.); constituents and phases (e.g. sodium, argon, etc.); geometrical configurations, phase topology, and/or flow regime (e.g. pool, bubble, etc.); fields (i.e. mass, moment, and energy); and transport processes. The final step in Element 1, Step 4, includes identification and ranking of key phenomena and processes with regard to their effect on the FOM identified in Step 2, or development of a phenomena identification and ranking table (PIRT). This PIRT will ultimately be used to guide overall EM adequacy assessment. This PIRT should utilize experimental data and sensitivity analyses to remove dependence on subjective expert opinion as possible, and the entire PIRT should be well documented in order to support the remainder of the EMDAP.

Element 2 of the EMDAP focuses on development of the assessment base against which the EM will be measured. Element 2 can be completed in parallel with Element 3. Step 5 (numbering continued from previous element), specification of objectives of the assessment base, includes development of a database that can be used for EM assessment. The database should include: separate effects experiments needed to assess correlations and closure models; integral systems tests needed to assess global code capability; benchmarks with other codes (optional); plant data (if available); and simple test problems that illustrate fundamental calculational capability. In Step 6, a scaling analysis to identify relevancy to the EM and similarity criteria is conducted for experiments identified during Step 5. In Step 7, the database developed at the beginning of Step 5 is supplemented with data from integral effects tests (IETs) and separate effects tests (SETs), and in Step 8 the IETs and SETs are reviewed for distortions or inconsistencies that result from scaling to the EM. The effects of these distortions are also identified in Step 8. The last step in Element 2 includes identification of relevant uncertainties in the database, and in particular, experiments, such as measurement errors or experimental distortions.

**Table 2.1: Key Elements of EMDAP [4]**

| Element Number | Title | Description |
|---|---|---|
| 1 | Establish Requirements for Evaluation Model Capability | 1. Specify analysis purpose<br>2. Specify figures of merit<br>3. Identify systems, components, phases, geometries, fields, and processes that should be modeled<br>4. Identify and rank phenomena and processes |
| 2 | Develop Assessment Base | 5. Specify objectives for assessment base<br>6. Perform scaling analysis and identify similarity criteria<br>7. Identify existing data and/or perform integral effects tests (IETs) and separate effects tests (SETs) to complete data set<br>8. Evaluate effects of IET distortions and SET scale-up capability<br>9. Determine experimental uncertainties |
| 3 | Develop Evaluation Model | 10. Establish EM development plan<br>11. Establish EM structure<br>12. Develop or incorporate closure models |
| 4 | Assess Evaluation Model Adequacy | 13. Determine model pedigree and applicability to simulate physical processes<br>14. Prepare input and perform calculations to assess model fidelity and/or accuracy<br>15. Assess scalability of models<br>16. Determine capability of field equates and numeric solutions to represent processes and phenomena<br>17. Determine applicability of EM to simulate system components<br>18. Prepare input and perform calculations to assess system interactions and global capability<br>19. Assess scalability of integrated calculations and data for distortions<br>20. Determine EM bases and uncertainties |

In Element 3 of the EMDAP, the EM itself is developed. Element 3 can be completed in parallel with Element 2, as they are independent processes. During Step 10 (numbering continued from Element 2), an EM development plan is established based on the requirements developed in Element 1. Components of the EM development plan closely resemble those of a conventional SQA Program, including the following verification-related activities and documents: a design specification for the calculational device; documentation requirements; programming standards and procedures; portability requirements; QA procedures; and configuration management procedures. Step 11, establishment of the EM structure, utilizes the characteristics identified in

Step 3 to construct the EM structure. As such, an EM structure should maintain the ability to analyze the behavior of all of the following characteristics at the relate to the intended end-use: systems and components; constituents and phases; field equations; closure relations; numerics (e.g. efficient and reliable calculations); and additional features (e.g. boundary conditions, control systems, etc.). In Step 12, closure models are developed or incorporated into the EM, as necessary. Closure models may be derived from SET or IET data, but the effects of scaling, the basis, range of applicability, and accuracy should be identified and documented.

The final portion of EMDAP, Element 4, focuses on evaluation of the adequacy of the EM. Element 4 utilizes two methodologies for EM evaluation: a "bottom-up" approach in steps 13-15 where the fundamental constituents of the EM and their validity/pedigree are examined, and a "top-down" approach in steps 16-19 where the capabilities and pedigree of the EM as an integrated product are examined. Steps 13-15 examine the validity and applicability of individual correlations, closure models, scaling, stability, convergence, and other fundamental EM properties. In Steps 16-19, plant transient data or IET data are utilized for an assessment of the broad capabilities and applicability of the EM. In Step 20, EM biases and uncertainties are identified, where the level of detail of this step is dictated by the output of Step 1, the purpose of the analysis. Some regulatory-related safety analyses require more robust uncertainty quantification and/or sensitivity studies built upon best estimates, whereas for others a simple conservative analysis may suffice.

At this point, a determination of the EM adequacy is made. If at any point throughout Element 4 unacceptable deficiencies are identified in the EM, a previous step should be revisited to correct the source of the issue. Note that requirements of the EM (Element 1) or the assessment base against which the EM is to be evaluated (Element 2) should not be arbitrarily changed to align with the EM. All changes, whether to EM requirements, the EM assessment base, or the EM itself, should be justified and documented.

SQA activities recommended by RG 1.203 include generalized best practices that are common to prevalent U.S. standards such as NQA-1 and DOE G 414.1-4. All activities completed as part of EMDAP should invoke SQA best practices, and primarily design control and review measures to ensure the EMDAP and its elements are appropriately documented, reviewed, and managed/controlled. Other SQA best practices that should be considered include procedural activities such as problem reporting and corrective actions, configuration management (including documentation control and records retention), independent reviews, development of user guidance, and overall traceability of all activities.

Development of various documentation throughout the EMDAP is prescribed by RG 1.203, where this documentation is meant to scope all elements in the EMDAP. The documentation, which should be controlled and maintained current at all times, is described below. Note that each document does not necessary apply to each element, although a particular document may be utilized throughout multiple elements.

- EM Requirements: The EM requirements developed in Element 1 should be clearly documented. These requirements will be utilized during the EM assessment. The requirements should reference or include in the relevant outcomes of the PIRT in whole or in part as part of requirements identification.

- EM Methodology: The interrelationship of all calculational devices in the EM, including input and output, for the specific transient of interest should be documented in a methodology summary or report. This methodology will be utilized during the actual EM application and should be reviewed during the EM assessment to ensure fulfillment of requirements and compliance with the assessment base.
- Calculational Device Description Manuals: All calculational devices (e.g. system software, simple spreadsheet, etc.) included in the EM must have an accompanying description manual. Descriptions should be included for the modeling theory, numerical schemes, architecture, and any other relevant attributes. Additionally, these manuals should be accompanied by a models and correlations quality evaluation report that provides information on the closure models, including: the source and quality; how the closure models are utilized in the EM; and a technical rationale for use of the closure models. These description manuals may be used during EM assessment.
- User's Manual and/or Guidelines: A User's Manual that describes how to prepare inputs and provides guidance on calculational model best practices should be developed for the EM and all of its calculational devices. Guidelines should include, but are not limited to: proper usage of the calculational device for the specific transient/accident under consideration; the range of applicability; calculational device limitations for the specific transient/accident under consideration; and recommended modeling options for the calculational device for the specific transient/accident under consideration. The Manual and guidelines are used during EM application.
- Scaling Reports: All scaling analyses that support the assessment base should be documented. These reports should be generated during development of the assessment base and are to be utilized during EM assessment.
- Assessment Reports: A series of assessment reports should be generated during EM assessment, including: a developmental assessment report that describes the EM's capability to treat a specific set of phenomena; a component assessment report that describes the abilities and assessment of any component-level calculational devices utilized in the EM; and IET assessment reports that describe and assess the overall EM's ability to treat integral behavior. In general, the assessment reports should address the following items:
    - Calculational device capability, including quantification of accuracy for parameters of interest;
    - Sensitivity and scaling analyses to determine whether results are affected by compensating errors;
    - Self-consistency of results supported by technically rational, acceptable, and cohesive information;
    - Agreement of timing of events determined by EM with experimental database;
    - Ability of EM to scale to prototypical conditions; and
    - Explanation of any unanticipated or unintuitive results;

  - Discussion of disagreement with experimental data (if any), including: identification of the source of the discrepancy, its significance, and description of why a potential deficiency may have a negligible effect for the scenario in question.
  - Discussion of input model and associated sensitivity study details, including: nodalization diagram and rationale; boundary, initial, and operational conditions; results of sensitivity studies on closure models or other parameters; modification to input model that result from sensitivity studies; and numerical convergence studies, including time step and convergence criteria bases.
- Uncertainty Analysis Reports: Any uncertainty quantification performed during Step 20 should be described and documented. The uncertainty analysis is used to assist with EM assessment.

## 2.2 ASME NQA-1 2008/2009 Standard

Developed and maintained by the American Society of Mechanical Engineers (ASME), the NQA-1 Standard sets forth requirements for the design and implementation of QA programs that are to be utilized throughout the lifetime of a nuclear facility, beginning with siting and design and ending with decommissioning. Despite the availability of more recent versions of the NQA-1 standard, the U.S. NRC formally endorses NQA-1-2008 [2] with the NQA-1a-2009 addendum[1] [3] in Regulatory Guide 1.28 "Quality Assurance Program Criteria (Design and Construction)" [5][2].

Requirements and sections of NQA-1-2008/2009 relevant to computer software include:

- Part I, Requirement 3: Design Control,
- Part I, Requirement 11: Test Control,
- Part II, Subpart 2.7: Quality Assurance Requirements for Computer Software for Nuclear Facility Applications,
- Part II, Subpart 2.14: Quality Assurance Requirements for Commercial Grade Items and Services,
- Part III, Subpart 3.3, Nonmandatory Appendix 3.1: Guidance on Qualification of Existing Data, and
- Part IV, Subpart 4.1: Application Appendix: Guide on Quality Assurance Requirements for Computer Software.

Details of Requirements 3 and 11 and select paragraphs of Subpart 2.7, Subpart 2.14, and Nonmandatory Appendix 3.1 are provided in Table 2.2 through Table 2.6. Details on Subpart 4.1 are not provided here. Particular focus should be given to Part II, Subparts 2.7 and 2.14, as

[1] Collectively referred to as the NQA-1-2008/2009 standard.
[2] It is the license applicant's responsibility to be aware of the standards and/or requirements endorsed by the regulator. In some cases, deviations from compliance with endorsed standards/requirements may be acceptable if sufficient justification is provided by the applicant.

the requirements in these subparts scope software verification in its entirety. Subpart 2.14 is particularly relevant as it outlines the requirements for software dedication. Requirements 3 and 11 of Part I should be used in conjunction with Subparts 2.7 and 2.14. Part III, Subpart 3.3, Nonmandatory Appendix 3.1 should be utilized when performing validation of software using data or alternative calculations of an indeterminate pedigree.

**Table 2.2: Summary of NQA-1-2008/2008 Requirement 3: Design Control [2, 3]**

| Paragraph | Title | Summary |
|---|---|---|
| 100 | Basic | The design shall be defined, controlled, and verified. Design adequacy shall be independently verified. Design interfaces and changes shall be governed by control measures. |
| 200 | Design Input | *See section 800.* |
| 300 | Design Process | *See section 800.* |
| 400 | Design Analyses | Design analyses shall be sufficiently detailed such that the analysis can be reviewed and verified by a technically qualified subject matter expert without recourse to the originator. |
| 401 | Use of Computer Programs | Computer program acceptability shall be preverified or the results verified with the design analysis for each application. Preverified computer programs shall be controlled in accordance with the requirements of this Standard.<br>(a) The computer program shall be verified to show that it produces correct solutions for the encoded mathematical model within defined limits for each relevant parameter.<br>(b) The encoded mathematical solution shall be shown to produce a valid solution to the physical problem associated with the particular application. |
| 402 | Documentation of Design Analyses | Documentation of design analyses shall include: (a) objective of the analysis; (b) design inputs and their sources; (c) applicable background information; (d) assumptions and related verification of assumptions; (e) identification of any supporting computer calculation; and (f) review and approval. |
| 500 | Design Verification | *See section 800.* |
| 600 | Change Control | *See section 800.* |
| 700 | Interface Control | Interface controls shall include establishment of procedures for review, approval, release, distribution, and revision of documents involving design interfaces. Design information shall identify the status of the transmitted item(s). |
| 800 | Software Design Control | Requirements of section 800 apply to computer software design control and shall be used instead of sections 200, 300, 500, and 600. |
| 801-801.5 | Software Design Process | The software design process shall be documented, approved, and controlled.<br>**Identification of Software Design Requirements:** Software requirements shall be identified and documented and their selection reviewed and approved. Software requirements shall identify the operating system, function, interfaces, performance requirements, installation considerations, design inputs, and any design constraints.<br>**Software Design:** The software design shall be documented and shall define the design necessary to meet software requirements. |

| Paragraph | Title | Summary |
|---|---|---|
| | | **Implementation of the Software Design:** The software design shall be implemented using documented programming standards and conventions.<br>**Software Design Verification:** Design verification shall be performed by a competent individual(s) other than those who developed and documented the design. Methods and results of design verification shall be documented. Acceptable verifications methods any one or combination of: design reviews, alternate calculations, and tests performed during development.<br>**Computer Program Testing:** Testing shall be performed in accordance with Requirement 11. |
| 802-802.3 | Software Configuration Management | **Configuration Identification:** Software configuration identification requires establishment of a software baseline and use of a labeling system for configuration items (CI) that identifies each CI, identifies changes to CIs by revision, and provides the ability to identify each configuration of the software available for use.<br>**Change Control:** Changes to software shall be controlled and documented; documentation shall include a description for the change, rationale for the change, and identification of affected baseline. The change shall be formally evaluated and approved and only authorized changes shall be made to a baseline. Appropriate verification and acceptance activities shall be performed for the change. The change shall be documented and traceable.<br>**Configuration Status Control:** The status of CIs shall be maintained current. CI changes shall be controlled until incorporated into the baseline. Controls shall include a process for maintains the status of changes that are proposed and approved, but not yet implemented. These controls shall also provide for affected user notification. |
| 900 | Documentation and Records | Design documentation and records shall include final documents, all revisions to these documents, and documentation related to important steps in the design process and sources of design inputs. |

**Table 2.3: Summary of NQA-1-2008/2008 Requirement 11: Test Control [2, 3]**

| Paragraph | Title | Summary |
|---|---|---|
| 100 | Basic | Tests shall be planned and executed, characteristics to be tested and test methods shall be specified, and tests results and their conformance with requirements and acceptance criteria shall be evaluated. |
| 200 | Test Requirements | (a) Test requirements and acceptance criteria shall be provided or approved by the design organization. Required tests shall be controlled. Tests performed shall obtain the data necessary for evaluation and acceptance.<br>(b) Test requirements and acceptance criteria shall be based upon specified requirements.<br>(c) If temporary changes are required for testing purposes, approval by the design authority is required prior to testing. |
| 300 | Test Procedures (Other than for Computer Programs) | *See section 400.* |

| Paragraph | Title | Summary |
|---|---|---|
| 400 | Computer Program Test Procedures | *The requirements of section 400 of Requirement 11 apply, instead of section 300, to testing of computer programs.*<br><br>(a) Test procedures shall provide for demonstration of adherence of the program to documented requirements. For programs used in design activities, test procedures shall provide for assurance the program produces correct results. For programs used for operational control, test procedures shall provide for demonstration of the required performance over the range of operation. Test procedures shall also provide for evaluation of technical adequacy through comparisons.<br><br>(b) In-use test procedures shall be developed and documented that permit demonstration of acceptable performance of the program in the operating system. In-use testing shall be performed after installation or when there are significant changes in the operating system. Periodic in-use manual or automatic self-checking in-use tests shall be prescribed and performed. |
| 500 | Test Results | Test results shall be documented and evaluated by a competent authority to ensure requirements have been satisfied. Test results for design qualification tests and software design verification shall be evaluated by the design organization. |
| 600 | Test Records | Test records shall be established and maintained to indicate the ability of the program to satisfactorily perform its intended function or meet its documented requirements. Minimum documentation can be found in para. 601 and 602. |
| 601 | Test Records | *N/A for computer programs.* |
| 602 | Computer Program Test Records | **Verification Test Records:** (1) computer program tested, (2) computer hardware tested, (3) test equipment and calibrations, where applicable, (4) date of test, (5) tester or data recorder, (6) simulation models used, where applicable, (7) test problems, (8) results and applicability, (9) action taken in connection with any deviations noted, (10) person evaluating test results.<br><br>**In-Use Test Records:** (1) computer program tested, (2) computer hardware tested, (3) test equipment and calibrations, where applicable, (4) date of test, (5) tester or data recorder, (6) acceptability. |

**Table 2.4: Summary of Select Paragraphs of NQA-1-2008/2008 Part II, Subpart 2.7 [2, 3]**

| Paragraph | Title | Summary |
|---|---|---|
| 200 | General Requirements | Software engineering (SE) elements include: (a) software acquisition methods, (b) software engineering methods used to manage life-cycle activities, (c) application of standards and conventions, (d) control of support software. |
| 201 | Documentation | The SE elements shall define the baseline documents that are to be maintained as records. |
| 202 | Review | Reviews of software shall ensure compliance with the approved software design requirements. Two types of reviews are required: consideration of the requirements related to preparation of the computer program for acceptance testing, and assurance of the satisfactory completion of the software development cycle including acceptance testing. Both reviews may be combined with design verification. |

| Paragraph | Title | Summary |
|---|---|---|
| 203 | Software Configuration Management | (a) The appropriate SE elements shall identify when baselines are to be established. Configuration items include: (1) documentation, (2) computer program(s), and (3) support software.<br><br>(b) The software configuration change control process shall include: (1) initiation, evaluation, and disposition of a change request, (2) control and approval of changes prior to implementation, (3) requirements for retesting and acceptance of the test results. |
| 204 | Program Reporting and Corrective Action | Methods for documenting, evaluating, and correcting software problems shall describe the evaluation process for determining whether a reported problem is an error or other type of mistake, and define the responsibilities for disposition of the problem reports. When the problem is determined to be an error, how the error relates to the SE elements, how the error impacts past and present use of the computer program, how the corrective action impacts previous development activities, and how users are notified of the error, its impact, and how to avoid the error shall be part of the method. |
| 300-302 | Software Acquisition | Procured software not approved under a program consistent with NQA-1 requirements shall undergo an evaluation to determine its compliance with Subpart 2.7. The determination shall be documented and shall identify: (a) capabilities and limitations for intended use, (b) test plans and tests cases required to demonstrate the capabilities within the limitations, and (c) instructions for use within the limits of the capabilities. Results of the determinations shall be reviewed and approved. |
| 400 | Software Engineering Method | SE methods shall be documented, and shall ensure that software life cycle activities are planned and performed in a traceable and orderly manner. |
| 401 | Software Design Requirements | Software design requirements shall address technical and software engineering requirements, which shall be traceable through the life cycle. |
| 402-402.1 | Software Design | The software design shall consider the program's operating environment, and measures to mitigate the consequences of problems shall be an integral part of the design. Software design verification shall evaluate the technical adequacy of the design approach and ensure completeness, consistency, clarity, and correctness of the software design, and shall verify that the design is traceable to the requirements. Design verification shall include the review of test results, and shall be completed prior to approval of the computer program for use. |
| 403 | Implementation | The implementation process shall result in software products such as program listings and instructions for use, and shall be reviewed in accordance para. 202. |
| 404 | Acceptance Testing | Acceptance testing shall demonstrate that the computer program meets all specified software design requirements. Acceptance testing shall demonstrate that the program: (a) properly handles abnormal conditions and credible failures, (b) does not perform adverse unintended functions, and (c) does not degrade the system. Acceptance testing shall be performed prior to approval for use and shall be planned and performed for all design requirements. Test plans, test cases, and test results shall be documented, reviewed, and approved. |

| Paragraph | Title | Summary |
|---|---|---|
| 405 | Operation | The implementation process shall result in software products such as program listings and instructions for use, and shall be reviewed in accordance para. 202. |
| 406 | Maintenance | The SE elements shall define how changes to software are controlled. Typically changes are in response to: (a) enhancement requests, (b) revisions based on software design requirements, (c) changes to the operating environment, (d) reported problems that must be corrected. |
| 407 | Retirement | During retirement, support for the software is terminated, and the routine use of the software shall be prevented. |
| 500 | Standards, Conventions, and Other Work Practices | The SE method or software acquisition method shall establish the standards, convention, and other work practices necessary to facilitate software life cycle activities. Standards, conventions, and other required work practices shall be documented. |
| 600 | Support Software | Support software includes software tools and system software. The SE method, software acquisition method, or both shall establish the need for software tools. |
| 601 | Software Tools | Software tools shall be evaluated, reviewed, tested, and accepted for us and placed under configuration control. Changes to the software tool shall be evaluated for impact on the software product to determine the level of review and retesting necessary. |
| 602 | System Software | System software shall be evaluated, reviewed, tested, and accepted for use as part of the software development cycle and shall be placed under configuration change control. Changes to system software shall be evaluated for impact on the software product to determine the level of reviews and resting required. |

**Table 2.5: Summary of Select Paragraphs of NQA-1-2008/2008 Part II, Subpart 2.14 [2, 3]**

| Paragraph | Title | Summary |
|---|---|---|
| 100 | General Requirements | Subpart 2.14 supplements the requirements of Part I and shall be used in conjunction with the applicable sections of Part I. |
| 300 | Utilization | Controls shall be implemented to ensure the procured item is adequate for its intended safety function. A dedication plan shall document and direct the controls and dedication activities. Only items that perform a safety function shall be considered candidates for dedication. |
| 400 | Technical Evaluation | A technical evaluation shall be performed to ensure the design requirements are appropriate for the intended safety function. Credible failure modes and the effects of the failure modes on the safety function should be considered in the technical evaluation and selection of critical characteristics. |
| 500 | Critical Characteristics | Identification of critical characteristics is a design activity that is dependent on the complexity, application, function, and performance of the item for its intended safety function. Critical characteristics to be considered for acceptance include part number, identification markings, and performance characteristics. Technical information, testing, quality assurance programs, etc., developed and/or supplied by the manufacturer shall be considered in the selection of critical characteristics and related acceptance criteria. In cases where the critical characteristics and acceptance criteria cannot be determined from the manufacturer's documentation, the dedicating entity may perform an |

| Paragraph | Title | Summary |
|---|---|---|
| | | engineering evaluation, examination, or test of the original item to develop appropriate critical characteristics and acceptance criteria. |
| 600 | Methods of Accepting Commercial Grade Items | The dedication method(s) shall provide a means to ensure that the commercial grade item meets the acceptance criteria specified for the identified critical characteristics. Selection of a dedication method(s) shall be based on the type of critical characteristics to be verified, available Supplier information, quality history, and degree of standardization. The dedicating entity is the organization that performs or directs the dedication activity and determines acceptance. |
| 601 | Special Test(s), Inspection(s), and/or Analyses | Special test(s), inspection(s) and/or analyses shall be conducted upon or after receipt of an item to verify conformance with the acceptance criteria, and may include post-installation testing. This method shall utilize sufficient data to develop the appropriate test(s), inspection(s), and/or analyses, including acceptance criteria. Interface with the Supplier may be necessary to obtain the required data, and data may also be developed by an engineering evaluation. |
| 602 | Commercial Grade Survey of the Supplier | A commercial grade survey may be utilized to verity that the processes and controls implemented by the Supplier on an item conform with the identified critical characteristics and acceptance criteria. The survey shall be specific to the scope of the particular commercial grade item being procured. The survey documentation shall provide evidence that processes and controls required for the critical characteristics were observed and evaluated for acceptance. |
| 603 | Source Verification | Source verification may be utilized at the Supplier's facility to verify the processes and controls implemented by the Supplier on the item conform with the identified critical characteristics and acceptance criteria. The scope shall include observations, examinations, performance tests, or final inspections, and shall also include verification of the Supplier's design, procurement, process, and control methods. Source verification documentation shall provide evidence that the Supplier's activities for the identified characteristics were observed and evaluated for acceptance. |
| 604 | Acceptable Supplier/Item/ Services Performance Record | Documentation of an acceptable performance record may be utilized to verify conformance with the identified characteristics and acceptance criteria. Acceptable forms of historical performance may be compiled from monitored performance of the item, product tests, certification to national codes/standards, and other industry records or databases. The acceptable performance record shall consider the condition of service, environmental condition, failure data, maintenance, testing, and any modifications. |
| 700 | Commercial Grade Services | Training, testing, software support, or other technical support may be provided as a commercial grade service. Service activities that alter or create new critical characteristics of an item that are used to determine the acceptability of the service that produced the critical characteristics shall not be considered a commercial grade service. |
| 800 | Documentation | Documentation of the dedication process shall be traceable to the item and shall include the following types of documents, depending on the applicable dedication method:<br>a) Dedication plans or procedures that include the essential elements of the dedication process<br>b) Commercial grade item procurement documents<br>c) Facility commercial grade definition criteria<br>d) Technical evaluation of the safety function<br>e) Critical characteristic identification and acceptance criteria |

| Paragraph | Title | Summary |
|---|---|---|
| | | f) Test reports or results, inspection reports, analysis reports<br>g) Commercial grade survey reports<br>h) Source verification reports<br>i) Historical performance information<br>j) Dedication report containing sufficient data to accept the item |

**Table 2.6: Summary of Select Paragraphs of NQA-1-2008/2009 Nonmandatory Appendix 3.1 [2, 3]**

| Paragraph | Title | Summary |
|---|---|---|
| 100 | General | This appendix provides nonmandatory guidance on qualification of existing data, including data of indeterminate quality. Existing data is defined as data determined to be necessary for activities specified in Part I, but developed outside the scope of NQA-1. |
| 301 | Data Qualification Planning | Qualification planning includes: (a) the reason(s) for qualifying the data, (b) the selected qualification method(s), (c) the rationale for selecting the methods, (d) the evaluation criteria, (e) description of required subject matter discipline experts, (f) identification of individuals performing qualification and their qualifications, (g) schedule for completing work. |
| 303 | Data Qualification Attributes | Attributes of data to consider during qualification include: (a) technical adequacy of equipment and procedures used to collect and analyze data, (b) the extent to which the data demonstrate the properties and ranges of interest, (c) conditions under which the data were obtained, (d) quality and reliability of the measurement control program under which the data were generated, (e) extent to which under which the data were generated may generally meet NQA-1 requirements, (f) prior uses of the data and associated verification processes, (g) prior peer reviews of data and their results, (h) extent and reliability of the documentation associated with the data, (i) extent and quality of corroborating data or confirmatory test results, (j) degree to which independent audits of the process the generated the data were conducted. |
| 400 | Qualification Methods | One or more of the following qualification methods should be used: (a) Quality Assurance Program Equivalency, (b) Data Corroboration, (c) Confirmatory Testing, (d) Peer Review. |
| 500 | Documentation of Results | Results should be documented in a report that includes: (a) scope of the task, (b) data set(s) for qualification, (c) expertise of individuals performing qualification, (d) method(s) of qualification and rationale for selected method(s), (e) evaluation criteria, (f) qualification criteria, (g) data generated by evaluation (if applicable), (h) the results of the evaluation, and (i) recommendation for/against changing the qualification status of the data. |

## *2.3 EPRI Technical Report 3002002289*

The Electric Power Research Institute (EPRI) developed Technical Report (TR) 3002002289, "Plant Engineering: Guideline for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications" [6], to provide guidance to the commercial nuclear industry on dedication of design and analysis safety-related software. This guidance helps vendors fulfill U.S. federal requirements on dedication of commercial-grade items that are not developed or pedigreed in accordance with an acceptable SQA

Program. This commercial-grade dedication (CGD) process is not necessarily a substitute for EMDAP (which examines both the software and the model/input), but rather should be considered a framework for an acceptance process that ensures the software will perform its intended function. EPRI TR 3002002289 formally defines dedication as the "acceptance process undertaken to provide reasonable assurance that a commercial-grade item to be used as a basic component will perform its intended safety function, and in this respect, is deemed equivalent to an item designed and manufactured under a 10CFR50 App. B QA program" [6]. It is assumed that the applicability of the software (e.g. can this software model this transient with sufficient fidelity?) has been determined prior to dedication. Key elements of CGD technical evaluation include:

- Safety function identification for the software being dedicated;
- Critical characteristic identification to assist with verification of the software's capabilities;
- A failure modes and effects analysis (FMEA) for the software to determine failure modes or mechanisms that could affect its ability to perform the safety function(s);
- Establishment of acceptance criteria for all critical characteristics;
- Identification of acceptance or verification methods/activities; and
- Documentation of the technical evaluation and acceptance assessment.

Acceptance methods verify fulfillment of the identified critical characteristics and ensure the software can perform its intended function. Four acceptance methods are identified in EPRI TR 3002002289:

- Method 1 – Inspection, test, or analysis performed after delivery;
- Method 2 – Commercial-grade survey;
- Method 3 – Product or process inspection at the supplier's facility; and
- Method 4 – Evaluation of historical performance of the supplier and the software.

Useful guidance for determining product selection attributes, product identification attributes, and various critical characteristics is included in EPRI TR 3002002289, and are summarized in Appendix A. Examples and descriptions of relevant critical characteristics or attributes per category, as well as high-level acceptance criteria and verification methods for each critical characteristic or attribute are also provided in Appendix A. Product selection attributes (Table A.1) describe the characteristics the software must possess to fulfill its intended end-use. These selection attributes can be used during the product selection (during an applicability evaluation) or product design, and therefore can be considered requirements of the software. Product identification attributes (Table A.2) are used to identify the software configuration and therefore can be considered an important component of configuration control and identification. Properties such as build number, revision, version number, etc. should be considered as part of product identification. Critical characteristics include those related to performance (Table A.3) and dependability (Table A.4). Performance critical characteristics describe the functionality of the code, e.g. quantification of output precision/tolerance/accuracy, input and output interfaces, and completeness and correctness of the software's functionality. Dependability critical characteristics describe the built-in quality of the software and general examine the SQA processes applied to the software during development.

## 2.4 Qualification Requirements Matrix

As described above, an essential element at each major step of the evolutionary process leading to a regulatory acceptance of SAS4A/SASSYS-1 is the implementation of a comprehensive set of qualification studies in which code predictions are compared with test data. This process guarantees the EM predictive capability for the intended code application. It also ensures that this predictive capability is maintained as models are upgraded to address findings from previous qualification studies, new features are added to encompass a broader range of applications, and modification are completed that facilitate code usage.

Given the review of the requirements in [2-4, 6] provided in the preceding sections, a matrix of high-level qualification and dedication requirements has been developed in Table 2.7 for EM qualification. The EM qualification and/or dedication follows a systematic approach consisting of major elements, where each item is addressed in conjunction with critical characteristics. As per [4, 6], a key activity in qualification and dedication involves the identification of valid bounds for the mathematical models and EM inputs, although each activity is not necessarily required for all elements. As such, the applicability of identification of model and input bounds for all elements in Table 2.7 has also been indicated. This helps reduce the magnitude of the documentation effort that is required. Identification of the bounds of mathematical models provides documentation of the approved ranges for specific models (e.g. a particular correlation may only be valid over a well-defined range as per empirical findings) which will assist users with code applicability evaluation. In the case of identification of the bounds of model (user) inputs, this activity provides documentation of the ranges over which a particular mathematical model has been implemented in the code and may also include documentation of the ranges over which the model was tested. This will also support users with code applicability evaluation.

**Table 2.7: Evaluation Model Qualification Matrix**

| EM Qualification Element | Description | Model Bounds | Input Bounds |
|---|---|---|---|
| Analytical Benchmarks | Although analytical benchmarks pertain, in a general sense, to EM verification, these calculations are crucial in the qualification of the code. A set of analytical benchmark problems are developed to test the physical phenomena modeled by the EM. These benchmarks typically feature simple geometries and/or conditions such that it is possible to obtain analytical solutions to a known problem. The wide range of analytical benchmarks provides confidence that the physical phenomena are correctly implemented and the numerical algorithms are adequate. | X | |
| Separate Effect Tests (SET) | SETs refer to well-controlled tests that are specifically directed at the qualification of basic models, physical phenomena, and/or plant components. These tests can be categorized as follows:<br>1. Test cases chosen to characterize the most important basic models and correlations of the EM. These tests can be performed for a range of conditions and properties. As such, EM and correlation qualification is contingent upon test conditions.<br>2. Tests that provide a basis for evaluation of the ability of the EM to predict the performance of specific fast reactor components. A component test consists of experimental evaluations on plant components performed on an individual basis. If a new component type is introduced in the plant, a component qualification against that plant component performance is needed. | X | X |
| Integral Effects Tests (IET) | These tests consist of scaled simulations of a fast reactor. The primary purpose of these tests is to evaluate the integral system performance and the interaction between the various components in the system. These experiments reproduce concurrent multi-physical phenomena and multiple reactor components. These tests can either be performed on a scaled down model of a fast reactor, a subset of the fast reactor systems or the entire system of a nuclear reactor, including the reactor core, primary and intermediate heat transport system, decay heat removal systems, and the balance of plant. | | X |
| Standard Nodalization | These tests are based on the nodalization used for SAS4A/SASSYS-1 qualification against SET/IETs. Guidelines are developed for nodalization of the various fast reactor components and regions to test EM nodalization sensitivity for the qualification tests. These guidelines are to be used to develop a standard nodalization that is consistent with the nodalization used to evaluate individual models and phenomena. This nodalization is then used for all full-scale EM. | X | X |

# 3 Performance Critical Characteristics and Evaluation Model Acceptance Criteria

This section focuses on the identification of critical characteristics and evaluation model acceptance criteria as they relate to software performance and modeling capabilities. To that end, a set of cross-cutting phenomena relevant to SFR event sequences has been identified for the purpose of evaluating SAS4A/SASSYS-1 documentation with regard to the ability to support the qualification and dedication requirements outlined in Section 2. As transient phenomena will vary with reactor design, a generic SFR configuration has been defined in Section 3.1 based on a review of domestic SFR vendor designs. Given this generic design, common event sequences and the relevant cross-cutting phenomena are then identified in Section 3.2.

## *3.1 Domestic SFR Design Features Review*

This section provides an overview of SFR vendor designs with the aim of identifying components and systems common to all plants and establishing a generic SFR configuration. These features will then be considered in the identification and prioritization of event sequences relevant to a license application. While it is the intent to focus only on domestic vendor designs, it should be noted that many of these vendors have partnered with international organizations to facilitate design and commercialization of the plants. Despite this, all vendors considered here have engaged with Argonne in recent efforts on SFR safety analyses and use of the SAS4A/SASSYS-1 code via strategic partnerships or FOA awards, with the expectation that the software will be utilized in some capacity for licensing analyses. The overview provided here is limited to consideration of the heat generation and heat rejection mechanisms and is not meant to scope the entirety of the facility (e.g. fuel storage method, fuel handling systems, etc. are not discussed here).

As indicated by Table 3.1, all domestic vendors are considering a core utilizing metal alloy fuel and a pool-type primary configuration. In this system, unlike an LWR, the majority of primary system components (primary coolant pumps, intermediate and decay heat exchanges, etc.) are submerged in the primary pool (Figure 3.1 [7]). In this configuration, hot sodium exiting the core is discharged to an upper plenum or hot pool. Sodium from the hot pool then passes through the intermediate heat exchanger and into the cold pool. Multiple primary pumps then draw sodium from the cold pool and discharge it to the inlet plenum, where it then passes through the core again. Pool-type reactors are advantageous in that they are inherently protected from loss of coolant accidents as no penetrations exist in the primary and guard vessels below the primary sodium level.

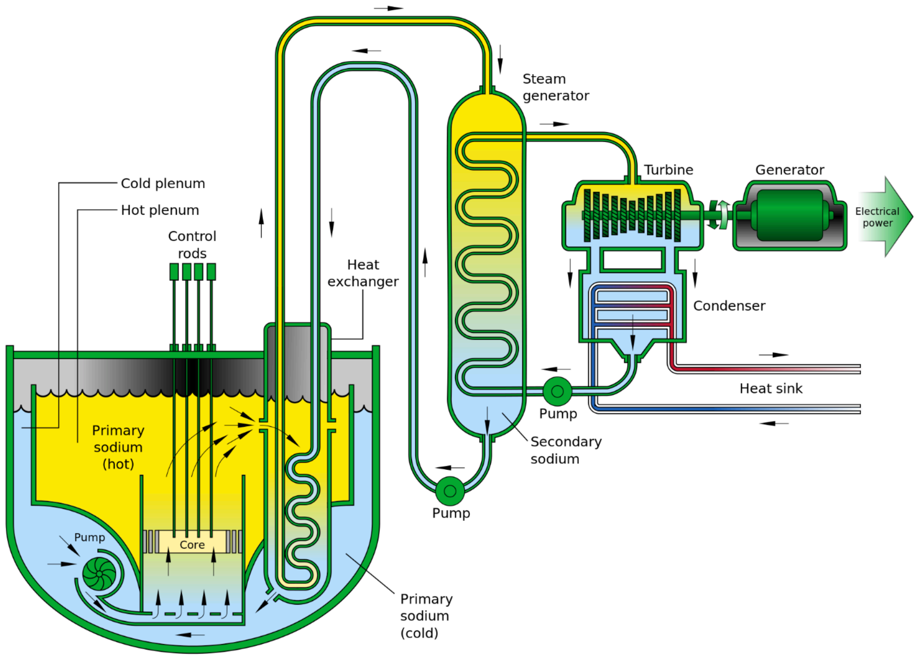


**Figure 3.1: Pool-type SFR Schematic [7]**

The reactivity of sodium with oxygen and water is managed by maintaining an inert cover gas region above the primary pool. The entire primary system vessel is sealed by an upper head, and the cover gas region (and therefore primary pool sodium) is typically maintained at approximately atmospheric pressures. The vessel head penetrations are limited to those necessary for fuel handling, intermediate heat transport system loops, decay heat removal system loops, instrumentation, or auxiliary systems (e.g. cover gas cleanup or sodium purification). The primary pool vessel is typically located below grade with a containment dome encapsulating the vessel head and some portion of the associated systems that penetrate the head.

The typical mechanism for primary system heat rejection is via an intermediate heat transport system (IHTS) which then rejects heat to a tertiary (typically steam) system. The IHTS also utilizes sodium and as such there is the possibility of sodium-steam interactions in the intermediate/tertiary loops. Decay heat removal systems range from heat exchangers submerged in the primary system (such as the direct reactor auxiliary cooling system (DRACS)) to reactor cavity cooling systems that remove heat from the guard vessel (such as the reactor vessel auxiliary cooling system (RVACS) utilized in GE-Hitachi's PRISM design), both of which operate by passive means.

A high-level summary of key design features for TerraPower's TWR-300, GE-Hitachi's PRISM, and ARC, LLC's ARC-100 designs is provided in Table 3.1. Based on the review provided here and information assembled in Table 3.1, the generic SFR design considered in this analysis is of a pool-type configuration utilizing metal alloy fuel. Due to the variation among the systems utilized in Table 3.1 for several key functions, only the phenomena related to that function will be considered in Section 3.2. For example, specific phenomena related to DRACS versus RVACS are not considered, only the high-level functionality (e.g. heat rejection due to passive operation) is considered. In an actual design-specific qualification or dedication activity, a more robust evaluation of phenomena directly relevant to these unique systems would be required. Event-specific phenomena can vary greatly for components and systems such as core shutdown and decay heat removal systems, spent-fuel storage, and pumps and should be considered carefully.

**Table 3.1: Selected Features for Domestic SFR Vendor Designs**

| Function/Feature | TWR (TerraPower) | PRISM (GE-Hitachi) | ARC-100 (ARC) |
|---|---|---|---|
| *Primary system configuration* | Pool | Pool | Pool |
| *Fuel type* | Metal alloy | Metal alloy | Metal alloy |
| *Core shutdown mechanisms* | Control rods<br>Reactivity feedback | Control rods<br>Reactivity feedback<br>Gas expansion modules (GEMs) | Control rods<br>Reactivity feedback |
| *Decay heat rejection* | DRACS<br>Draft HX | RVACS | DRACS |
| *Spent-fuel storage* | | In-vessel | |
| *Primary forced convection* | Mechanical pumps | Electromagnetic pumps | Mechanical pumps |

## *3.2 Event Sequence and Phenomena Identification*

In order to effectively assess the status of SAS4A/SASSYS-1 documentation as it relates to qualification, it is necessary to identify and prioritize the phenomena that are expected to be included in a licensing safety analysis. As such, given the generic reactor configuration and systems identified in Section 3.1, a series of event sequences has been identified for consideration. From these event sequences, cross-cutting phenomena can then be identified. In an effort to comprehensively address all relevant event sequences and phenomena, industry-developed PIRTs and the Sodium Fast Reactor Safety and Licensing Research Plan [8] have been reviewed as part of this effort.

As per the U.S. NRC's Standard Review Plan (SRP) [9], the rigor of the safety analysis varies depending on the event class (e.g. design basis, design extension, etc.), with analysis pedigree increasing with event series frequency. Therefore, this effort is limited to consideration of those events expected to be included in a Chapter 15 analysis of the SRP, which scopes events that are of moderate frequency (i.e. expected to occur several times during plant lifetime) and infrequent events (i.e. may occur during plant lifetime). In general, these tend to be single-fault events and do not result in fuel failure or large-scale coolant boiling[3]. This event sequence review scopes operational events only and therefore accidents that occur during fuel handling, fuel storage, or scenarios not related to normal operation are excluded from further

[3] Double-fault events could be included in a Chapter 15 analysis, depending on the results of a probabilistic risk assessment (PRA) and subsequent determination of the design basis accident(s). It is critical to note that meaningful event sequence classification cannot occur without development of a PRA.

consideration here. Sodium fire events are also excluded from further consideration here as the role of SAS4A/SASSYS-1 in analysis of these events is very limited.

All operational transients that occur in an SFR can be characterized by either undercooling or reactivity insertion. An undercooling event can occur as the result of full or partial loss of flow in the primary system (due to pump fault(s) or subassembly blockage(s)), loss of normal heat rejection pathways (due to pump fault(s) in the intermediate heat transport system or fault(s) in the power conversion system), or a station blackout in which forced flow is lost in all heat transport systems and all normal heat rejection pathways are lost. Reactivity insertion events can occur as the result of unplanned withdrawal of one or more control rods or overcooling of the system due to pump overspeed or faults in the power conversion system.

Because it is the intent of this effort to examine events primarily limited to single faults, it is assumed that the reactor shutdown system actuates successfully, resulting in a protected event sequence for the types of scenarios described above. Furthermore, the magnitude of the failures (e.g. number of faulted pumps or rate of control rod withdrawal) is not assessed here, as this analysis only qualitatively considers the event sequence space.

A summary of the event sequence and relevant phenomena evaluation can be found in Table 3.2 through Table 3.5 for loss of primary flow, loss of normal heat rejection, positive reactivity insertion due to rod withdrawal, and positive reactivity insertion due to overcooling transients, respectively. As the phenomena identified for individual event sequences is scoped by that expected to occur during a station blackout, no separate evaluation of a station blackout is included here. Phenomena not included in the capabilities of SAS4A/SASSYS-1 are highlighted in red in these tables.

**Table 3.2: Generic Events and Phenomena – Loss of Primary Flow Transients**

| Transient Description | Relevant Phenomena |
|---|---|
| *Loss of primary flow (undercooling)* | |
| Pump fault(s)<br>Subassembly blockage(s) | **Thermal hydraulic**<br>• Pump coastdown behavior<br>• Transition to natural circulation flow regime in primary system<br>• Core flow redistribution in loss of forced convection<br>• Asymmetric temperature/flow distribution in pools<br>• System-wide thermal inertia (structures, components, coolant)<br>• Pool stratification<br>• IHX outlet window stratification<br>• Decay heat generation<br>• Transition in natural circulation flow regime in passive decay heat removal systems<br>**Reactivity (prior to scram)**<br>• Reactivity feedback response due to thermal-geometry changes (axial fuel/clad, radial core, control rod drive expansion, vessel elongation)<br>• Reactivity feedback response due to thermal-neutronic changes (Doppler)<br>• Reactivity feedback response due to localized coolant voiding<br>• Decay heat generation<br>**Structural/Material**<br>• Steady-state fuel characterization (heat transfer, fission gas generation, constituent migration, irradiation-induced swelling etc.)<br>• Vessel, structure behavior at elevated temperatures<br>• Clad/fuel behavior at elevated temperatures<br>• Primary boundary integrity at elevated temperatures |

**Table 3.3: Generic Events and Phenomena – Loss of Normal Heat Rejection Transients**

| Transient Description | Relevant Phenomena |
|---|---|
| *Loss of normal heat rejection pathway (undercooling)* | |
| Intermediate pump fault(s)<br><br>Power conversion system fault(s) | **Thermal hydraulic**<br>• Transition to natural circulation flow regime in intermediate system<br>• System-wide thermal inertia (structures, components, coolant)<br>• Asymmetric temperature/flow distribution in primary pools<br>• Decay heat generation<br>• Transition in natural circulation flow regime in passive decay heat removal systems<br>**Reactivity (prior to scram)**<br>• Reactivity feedback response due to thermal-geometry changes (axial fuel/clad, radial core, control rod drive expansion, vessel elongation)<br>• Reactivity feedback response due to thermal-neutronic changes (Doppler)<br>• Reactivity feedback response due to localized coolant voiding<br>• Decay heat generation<br>**Structural/Material**<br>• Steady-state fuel characterization (heat transfer, fission gas generation, constituent migration, irradiation-induced swelling, etc.)<br>• Reactions (chemical, mechanical/pressure) due to secondary/tertiary loop coolant interactions<br>• Vessel, structure behavior at elevated temperatures<br>• Clad/fuel behavior at elevated temperatures<br>• Primary boundary integrity at elevated temperatures |

**Table 3.4: Generic Events and Phenomena – Positive Reactivity Insertion Transients (Rod Withdrawal)**

| **Transient Description** | **Relevant Phenomena** |
|---|---|
| *Positive insertion (rod withdrawal)* | |
| Unplanned withdrawal of control rod(s) | **Thermal hydraulic**<br>• System-wide thermal inertia (structures, components, coolant)<br>• Asymmetric temperature/flow distribution in primary pools<br>• Transition in natural circulation flow regime in passive decay heat removal systems<br>• Decay heat generation<br>**Reactivity (prior to scram)**<br>• Reactivity feedback response due to thermal-geometry changes (axial fuel/clad, radial core, control rod drive expansion, vessel elongation)<br>• Reactivity feedback response due to thermal-neutronic changes (Doppler)<br>• Reactivity feedback response due to localized coolant voiding<br>• Point kinetics<br>• Decay heat generation<br>**Structural/Material**<br>• Steady-state fuel characterization (heat transfer, fission gas generation, constituent migration, irradiation-induced swelling, etc.)<br>• Vessel, structure behavior at elevated temperatures<br>• Clad/fuel behavior at elevated temperatures<br>• Primary boundary integrity at elevated temperatures |

**Table 3.5: Generic Events and Phenomena – Positive Reactivity Insertion Transients (Overcooling)**

| **Transient Description** | **Relevant Phenomena** |
|---|---|
| *Positive insertion (overcooling)* | |
| Pump overspeed<br><br>Intermediate/tertiary heat transport system fault(s) | **Thermal hydraulic**<br>• System-wide thermal inertia (structures, components, coolant)<br>• Asymmetric temperature/flow distribution in primary pools<br>• Transition in natural circulation flow regime in passive decay heat removal systems<br>• Decay heat generation<br>**Reactivity (prior to scram)**<br>• Reactivity feedback response due to thermal-geometry changes (axial fuel/clad, radial core, control rod drive expansion, vessel elongation)<br>• Reactivity feedback response due to thermal-neutronic changes (Doppler)<br>• Point kinetics<br>• Decay heat generation<br>**Structural/Material**<br>• Steady-state fuel characterization (heat transfer, fission gas generation, constituent migration, irradiation-induced swelling, etc.)<br>• Vessel, structure behavior at elevated temperatures<br>• Clad/fuel behavior at elevated temperatures<br>• Primary boundary integrity at elevated temperatures |

With evaluation of event sequence phenomena complete, a prioritized list of cross-cutting phenomena can be created. The phenomena identified in Table 3.2 through Table 3.5 were assembled and ordered with respect to their relevance to the number of event sequences. Note that this is not a complete assessment of the actual relative importance of the phenomena among all events. For example, pump coastdown behavior is one of the most important factors in the outcome of a loss of flow transient with respect to fuel damage. However this characteristic is only relevant to one generic event sequence category in this assessment, and therefore it is considered of relatively low importance as the goal of this effort is to address the maximal number of event sequences. True importance should be assessed via phenomena identification and ranking tables (PIRTs) and sensitivity analyses. The results of the cross-cutting phenomena listing are found in Table 3.6. Phenomena not included the capabilities of SAS4A/SASSYS-1 are excluded from this list.

**Table 3.6: Listing of Cross-Cutting Phenomena for Generic Event Sequences**

| **Cross-Cutting Phenomena** |
|---|
| *Reactivity feedback response due to thermal-geometry changes (axial fuel/clad, radial core, control rod drive expansion, vessel elongation)* |
| *Reactivity feedback response due to thermal-neutronic changes (Doppler)* |
| *Reactivity feedback response due to localized coolant voiding* |
| *Decay heat generation (neutronic)* |
| *System-wide thermal inertia (structures, components, coolant)* |
| *Transition in natural circulation flow regime in passive decay heat removal systems* |
| *Decay heat generation (thermal)* |
| *Steady-state fuel characterization* |
| *Clad/fuel behavior at elevated temperatures* |
| *Transition to natural circulation flow regime in primary system* |
| *Point kinetics* |
| *Pump coastdown behavior* |
| *Core flow redistribution in loss of forced convection* |
| *Pool stratification* |

# 4 SAS4A/SASSYS-1

This section provides background on the SAS4A/SASSYS-1 code and the current status of items relevant to software qualification. Development of the SAS series of codes, which began in the mid-1960s to model the initiating phases of core disruptive accidents in SFRs, has historically existed in the R&D space. The initial iteration, SAS1A, originated as a sodium-boiling model that included single- and two-phase coolant flow dynamics, fuel and cladding thermal expansion and deformation, molten fuel dynamics, and a point kinetics model with reactivity feedback [10]. By 1974, SAS evolved into the SAS2A computer code [11] which included enhanced abilities to model the initiating phases of loss of flow (LOF) and transient overpower (TOP) accidents up to the onset of fuel and cladding motion and cladding failure.

The SAS3A code [12] added mechanistic models of fuel and cladding melting and relocation. This version of the code was used extensively for analysis of accidents in the licensing of the Fast Flux Test Facility (FFTF) and therefore underwent significant verification and validation that aligned with the software qualification practices of that time. In the late 1970s, SAS3A was completely rewritten and released as SAS3D [13] in an effort to address the need for improved code portability, maintainability, data management schemes, and runtimes.

The SAS4A version of the code [14], which included new fuel element deformation, disruption, and material relocation models in anticipation of the LOF and TOP analysis needs for the licensing of the Clinch River Breeder Reactor (CRBR) Plant, underwent extensive validation against TREAT M-Series test data [15]. In the mid-1980s, a variant of SAS4A, named SASSYS-1 [16] with the capability to model ex-reactor coolant systems was developed with the aim of simulating accident sequences involving or initiated by loss of heat removal or other coolant system events. While SAS4A and SASSYS-1 have historically been released and utilized as separate codes, they have always shared common code architectures, the same data management strategy, and the same core channel representation, and therefore the two code branches were merged into a single code referred to as SAS4A/SASSYS-1 in the late 1980s.

Revisions to SAS4A/SASSYS-1 continued throughout the Integral Fast Reactor (IFR) program between 1984 and 1994 [17] resulting in the completion of SAS4A/SASSYS-1 v 3.0 in 1994 [18]. In this time, the design and analysis emphasis shifted towards metallic fuel and accident prevention by means of inherent safety mechanisms. In terms of SAS4A/SASSYS-1 modeling improvements, this resulted in addition of new models and modification of existing models to treat metallic fuel, its properties, behavior, and accident phenomena, and addition and validation of new capabilities for calculating whole-plant design basis transients, with emphasis on the EBR-II reactor and plant [19]. The whole-plant dynamics capability of SASSYS-1 plays a vital role in predicting passive safety feedback as it enables deterministic identification of meaningful boundary conditions for the core channel models, which are required for reliable prediction of accident progression.

SAS4A/SASSYS-1 v 3.1 had been completed as a significant maintenance update by the mid 1900s, but it was not released until 2012 [20]. In the time since the development of Version 3, a variety of modeling additions and enhancements have been made to meet U.S. DOE programmatic needs. This collection of updates was released in 2012 as SAS4A/SASSYS-1 Version 5.0.

The remainder of this section is structured as follows: Section 4.1 provides an overview of the current capabilities of SAS4A/SASSYS-1 and its expected role in licensing. Section 4.2 describes the existing software quality assurance (SQA) program, Section 4.3 provides an overview of the current V&V status of the code, and the current state of documentation, particularly as it relates to software qualification, is described in Section 4.4.

## 4.1 Capabilities and Expected Role in Licensing

The SAS4A/SASSYS-1 code, a systems-level integrated analysis tool, maintains the capability to model the majority of steady state and transient phenomena anticipated to be relevant to SFR licensing. High-level functional areas that characterize the behavior of an SFR and the anticipated role SAS4A/SASSYS-1 would provide in analyses of these functional areas are defined in Table 4.1. Additional details on each functional area with regard to the specific behavior or phenomena can be found in [21], while details on the maturity of the various models in SAS4A/SASSYS-1 can be found in [8].

**Table 4.1: SAS4A/SASSYS-1 Capability Description**

| Functional Area | SAS4A/SASSYS-1 Capability* |
|---|---|
| *Steady-state fuel cycle and neutron transport* | *n/a* |
| *Steady-state fuel performance* | Supporting |
| *Core-wide thermal hydraulics* | Primary |
| *Fission gas behavior* | Primary |
| *In- and ex-pin fuel and clad motion* | Primary |
| *Sodium boiling* | Primary |
| *Primary/intermediate system heat transport* | Primary |
| *Structural response* | Primary |
| *Inherent reactivity feedback* | Primary |
| *Passive heat removal* | Primary |
| *Sodium-water interactions* | *n/a* |
| *Sodium fires* | *n/a* |
| *Control system response* | Primary |
| *System-wide power and flow transient analyses* | Primary |
| *Source term* | Supporting: Determines timing, magnitude, and location of fuel failure |

**Primary capability indicates results are produced directly by SAS4A/SASSYS-1, while supporting indicates SAS4A/SASSYS-1 results are utilized in subsequent calculations by a separate tool.*

## 4.2 SQA Program

The SAS4A/SASSYS-1 SQA Program structure has been developed with the goal of targeting the requirements found in DOE O 414.1D [22], DOE G 414.1-4 [23], and NQA-1-2008/2009 [2, 3]. The SQA Program applies to all activities related to the software life cycle of the SAS4A/SASSYS-1 code library and associated documentation and utilities. However, the application of SAS4A/SASSYS-1 to end-user needs with regard to suitability and quality is beyond the scope of the SAS4A/SASSYS-1 SQA Program, meaning users are responsible for ensuring that the software is sufficient for the specified task and that the appropriate SQA measures required by their respective organization are applied.

The remainder of this section will discuss the structure of the SQA Program, with focus on Program documentation. A hierarchical document structure has been adopted for the SAS4A/SASSYS-1 SQA Program, with a central SQA Plan (SQAP) comprising the top level of the Program. A brief description of each document is included below, and a graphical hierarchy is provided in Figure 4.1. The Program consists of a series of plans and procedures. While the purpose of procedures is to define the workflow for software development, testing, and release, the main outputs of procedures are the QA records that document the completion of tasks in the procedure workflow and that provide traceability for future review or audits.

- **Software Quality Assurance Plan (SQAP):** The Program's approach to SQA and an overview of all SQA Program activities and requirements are provided in the SQAP. This top-tier document acts as an entry point to the SQA Program and directs developers, managers/leaders, and SQA coordinators to the appropriate sublevel document for all Program activities. The primary purpose of the SQAP is to delineate the SAS4A/SASSYS-1 SQA Program framework by describing Program activities, organization, and documentation such that the interconnection of all Program items and activities is clearly defined. In addition to the guidance in [2, 3, 23], the requirements in IEEE Std 730-2002, "IEEE Std for Software Quality Assurance Plans" [24], were also referenced during SQAP development.
- **Configuration Management Plan (CMP):** The CMP describes the processes required for control of all configuration items in the SAS4A/SASSYS-1 SQA Program. This second-tier document provides details on the various CM activities that are inherent in all procedures, including revisioning of configuration items, repository access permissions, status accounting, configuration reviews, identification of configuration items, and formal release and delivery of products. The CMP defines configuration items (CIs) in the SAS4A/SASSYS-1 SQA Program to include: source code and associated makefiles, developer utilities (test scripts), data (test case input and reference output), user utilities (post-processing tools), and documentation (SRS, SDD, Program plans and procedures, SAS4A/SASSYS-1 Code Manual, and interface control documents). Configuration identification and control of CIs is accomplished via the electronic repository system Subversion (SVN) [25]. Configuration status accounting utilizes the electronic integrated CM and issue tracking system Trac [26]. In addition to the guidance in [2, 3, 23], the requirements in IEEE Std 828-2005, "IEEE Standard for Software Configuration Management Plans" [27] were also referenced during development of the CMP.
- **Coding Standards:** The Coding Standards (CS) document outlines the coding standards and programming practices which developers are required to follow. These requirements apply to all development and modification activities; changes to an established baseline cannot occur unless they adhere to this document. As the SAS4A/SASSYS-1 source code and its accompanying utilities contain both Fortran and C/C++, the appropriate ISO/IEC standards for these languages are identified in this

document. The CS document also contains an abbreviated list of required programming practices. These requirements, which are largely associated with programming style, are imposed primarily to improve code readability and reduce coding errors.

- **Procedures:** The following third-tier documents are utilized as procedures in the SAS4A/SASSYS-1 SQA Program:
    - **Problem Reporting and Corrective Action:** Defines steps for reporting, assessing, and correcting code or documentation errors. Also defines steps for completing minor tasks not associated with major development efforts.
    - **Software Development and Modification:** Defines steps for the design and implementation of new features or models, creation of the associated documentation, and review/approval of software modifications and associated documentation. In this procedure, software requirements and design are formally documented, resulting in the Software Requirements Specification (SRS) and Software Design Description (SDD).
    - **Software Testing:** Defines steps for evaluating whether software adequately performs all intended functions. In this procedure, software testing is formally documented, resulting in a Software Test Plan (STP) and reference input(s)/output(s).
    - **Version Release:** Defines steps for the formal release of software and delivery of products.

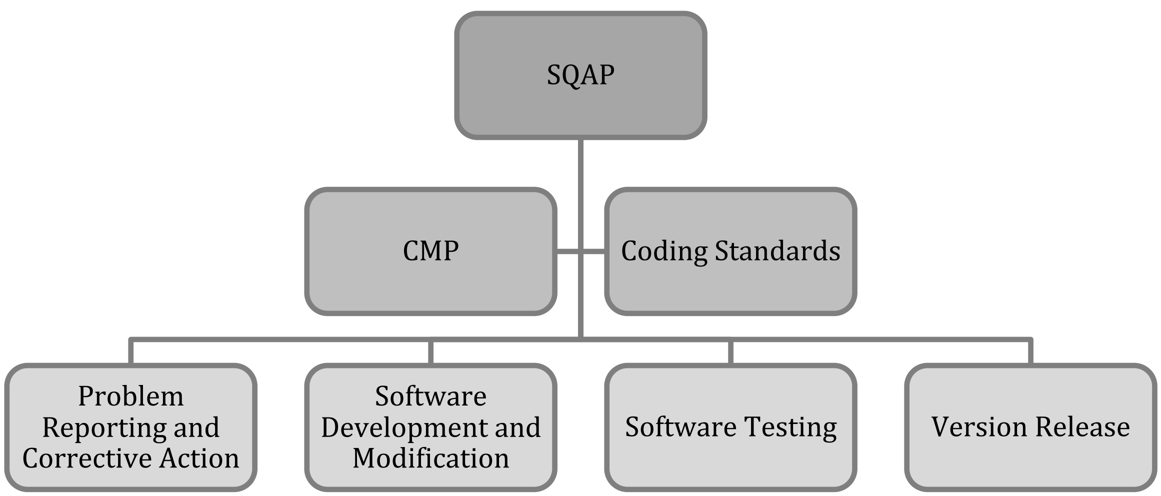


**Figure 4.1: Graphical Representation of SAS4A/SASSYS-1 SQA Program Hierarchy**

## 4.3 V&V Activities

### 4.3.1 V&V Test Suite

A series of verification test cases has been developed to exercise a broad range of basic steady-state and transient capabilities of SAS4A/SASSYS-1. Cases were constructed such that each subsequent test builds upon the previous, meaning the test cases increase in complexity. Analytical (typically spreadsheet) solutions have been derived for each test case. Computational results are considered acceptable if negligible error between the computational and analytical solutions are found for the metric(s) of interest. All test cases utilize sodium as the coolant and generic and/or simplified reactor parameters were utilized to minimize test case complexity. It should be noted that these test problems are considered to primarily be verification test problems. The methodology utilized for development of the Test Suite is briefly described in Table 4.2. A brief listing of cases included in the Test Suite is provided in Table 4.3.

**Table 4.2: V&V Test Suite Development Methodology**

| Step | Activities |
|---|---|
| Define test | Develop test problem definition. The objective(s) of the test, key input parameters, output metrics of interest, and acceptance criteria for the test problem should be documented. Any initial conditions or clarifying assumptions should also be stated. |
| Develop analytical solution | Develop and document an analytical solution which may be based on a system of first principles and implemented via a spreadsheet or hand calculation. Simplified numerical solutions for more complex models are also acceptable. The solution should meet the objectives of the test, utilize the defined input parameters, and produce the relevant output metrics. Any additional assumptions necessary to compute the solution should also be clearly stated. At this stage, it may be necessary to choose algorithms or solution schemes that match limitations of the software (e.g. implementation of a linear approximation instead of exact solution or use of particular meshing scheme). |
| Create SAS4A/SASSYS-1 solution | Develop and document a model and corresponding code input and generate a corresponding computational solution. The model should be designed and built as per the problem definition in the first step. The solution should meet the objectives of the test, utilize the defined input parameters, and produce the relevant output metrics. Any additional assumptions necessary to produce the solution should also be clearly stated. It should be ensured that the assumptions and solution schemes used in the computational and analytical solutions are consistent. |
| Compare solutions | Compare the analytical and computational solutions. Satisfaction of acceptance criteria should be reviewed and documented. Deviations from the acceptance criteria can be accepted if appropriate justifications are developed. For cases that do not satisfy acceptance criteria, generate a problem report. |

**Table 4.3: Listing of SAS4A/SASSYS-1 V&V Test Suite Cases**

| Case | Description |
|---|---|
| | **Simple Steady-State Cases** |
| 1.1 | Base test case |
| 1.2 | Increasing the number of pins |
| 1.3 | Increasing the number of assemblies |
| 1.4 | Increasing the number of core channels |
| 1.5 | Adding 3 lower reflectors and 3 upper reflectors with an upper fission gas plenum |
| 1.6 | Adding 3 lower reflectors and 3 upper reflectors with a lower fission gas plenum |
| 1.7 | Adding 1 lower reflector and 5 upper reflectors |
| 1.8 | Adding 5 lower reflectors and 1 upper reflector |
| 1.9 | Form loss pressure drop in the channel |
| | **Simple Transient Cases** |
| 2.1 | Maintaining steady-state temperatures during the transient |
| 2.2 | Increasing reactor power |
| 2.3 | Increasing core inlet temperature |
| 2.4 | Decreasing sodium mass flow rate |
| | **Material Properties Cases** |
| 3.1 | Using the temperature-dependent sodium density |
| 3.2 | Using the temperature-dependent sodium heat capacity |
| 3.3 | Using the temperature-dependent sodium thermal conductivity and convective heat transfer coefficient |
| 3.4 | Using the temperature-dependent cladding thermal conductivity |
| 3.5 | Using the temperature-dependent fuel thermal conductivity |
| 3.6 | Using the temperature-dependent built-in sodium properties |
| | **Core Power Cases** |
| 4.1 | Sinusoidal power axial profile |
| 4.2 | Point kinetics vs. user-defined total power |
| 4.3 | Old decay heat model with one group |
| 4.4 | Old decay heat model with six groups |
| 4.5 | New decay heat model with six groups |
| 4.6 | ANS decay heat standard using new decay heat model |
| 4.7 | ANS decay heat standard model |
| 4.8 | Combination of new decay heat model and ANS decay heat standard model |
| 4.9 | External reactivity insertion at zero power |
| 4.10 | External reactivity insertion at full power |
| 4.11 | Doppler reactivity feedback |
| 4.12 | Axial fuel expansion reactivity feedback |
| 4.13 | Axial cladding expansion reactivity feedback |

| Case | Description |
|---|---|
| 4.14 | Axial fuel and cladding expansion reactivity feedback, independent expansion option |
| 4.15 | Axial fuel and cladding expansion reactivity feedback, clad-based option |
| 4.16 | Axial fuel and cladding expansion reactivity feedback, force balance option |
| 4.17 | Axial structure expansion reactivity feedback |
| 4.18 | Sodium void reactivity feedback |
| 4.19 | Modeling feedbacks on the MZ and MZC meshes |
| 4.20 | Control rod driveline expansion reactivity feedback |
| 4.21 | Vessel expansion reactivity feedback |
| 4.22 | Radial core expansion reactivity feedback |
| **Heat Removal Systems Cases** | |
| 5.1 | Steady-state PRIMAR-4 temperatures |
| 5.2 | Maintaining PRIMAR-4 temperatures during the transient |
| 5.3 | User-defined temperature drop simple IHX model |
| 5.4 | User-defined outlet temperature simple IHX model |
| 5.5 | Detailed IHX model |
| 5.6 | Introducing a second heat exchanger |
| 5.7 | Friction pressure drop |
| 5.8 | Bends pressure drop |
| 5.9 | Form loss pressure drop |
| 5.10 | Gravity pressure drop |
| 5.11 | Acceleration pressure drop |
| 5.12 | Steady-state pump head |
| 5.13 | Valve loss coefficient |
| 5.14 | User-defined temperature drop simple steam generator model |
| 5.15 | User-defined outlet temperature simple steam generator model |
| 5.16 | Equilibrating to and maintaining new temperatures in a transient |
| 5.17 | Heat transfer between an element and a constant temperature external heat source |
| 5.18 | Heat transfer between a compressible volume and a constant temperature external heat source |
| 5.19 | Natural circulation without orifice coefficients or pipe bends |
| 5.20 | Natural circulation with form loss pressure drops |
| 5.21 | Natural circulation with bends pressure drop |
| 5.22 | Core reference elevation |
| **Control System Cases** | |
| 6.1 | Block signals (simple mathematical and logic), demand table signals, time signal |
| 6.2 | Dynamic block signals |
| 6.3 | HTS temperature and density measured signals |
| 6.4 | HTS pressure and flow measured signals |

### 4.3.2 Legacy Validation of Severe Accident Modules

Rapid updates to SAS4A/SASSYS-1 occurred in the early 1970s with inclusion of mechanistic treatment of slug/bubble coolant boiling models in SAS2A and oxide fuel/cladding melting and relocation in SAS3A via addition of the CLAZAS, SAS/FCI, and SLUMPY modules. In the early 1980s, the severe accident modules underwent significant revisions as part of the update to SAS4A. The clad/fuel movement/relocation modules CLAZAS, SAS/FCI, and SLUMPY of SAS3A/SAS3D[4], which treated the phenomena sequentially, were replaced with the CLAP, PLUTO2, and LEVITATE modules in SAS4A, which enabled loose coupling of clad and fuel movement. In the late 1970s and early 19080s, the FPIN2 module, which treats metallic fuel/cladding fuel element mechanics, and DEFORM-4 and DEFORM-5 modules[5], which treat oxide and metal fuel/cladding mechanics and pin failure, were added to SAS4A.

As licensing of FFTF extensively used SAS3A for accident analyses, and SASSYS and the severe accident modules of SAS3A and SAS4A were expected to be used for licensing of CRBR, these codes underwent significant validation through the 1970s and 1980s to develop confidence in the codes' modeling capabilities. Most validation activities utilized the transient overpower (TOP) or transient undercooling (TUC) tests performed at the Transient Reactor Test Facility (TREAT) on oxide and metal fuel. Table 4.4 below provides a listing of the experiments utilized for validation, the relevant code version and module, and brief test description. This listing has been developed based on recovered, existing validation documentation and does not necessary reflect all historical validation efforts. Additionally, this table does not include validation of the SASSYS-1 RVACS module using data generated at Argonne's RVACS/RACS experimental facility or the SASSYS-1 validation studies completed in the 1980s based on FFTF passive safety experiments.

Due to lapses in resource maintenance and periodic updates in legacy data storage/retention, code input structure, and code input format (e.g. physical cards versus digital input files), nearly all input decks that support these validation cases are no longer available. Most historical SAS3D validation efforts have limited applicability to the current version of the code due to the significant severe accident module updates as part of SAS4A. Additionally, while historical validation activities have been well-documented qualitatively, software quality assurance and V&V practices and requirements have evolved significantly since that time in complexity and scope.

Despite this, several legacy input files have been recovered, including:

- SAS3D validation using the L6 and L7 LOF tests in TREAT,
- SAS4A validation using the RFT-L1, L03, TS-1, and TS-2 TOP tests in TREAT, and
- SAS4A validation using the L07 TOP-driven LOF in TREAT.

Several input decks that are assumed to represent FPIN2 validation against the M5, M6, and M7 metallic-fuel TREAT tests are also available, however documentation of comparisons of

[4] SAS3D was completed in the late 1970s as a major rewrite of SAS3A to address code portability, runtime, and data management. No new phenomenological models were added as part of this update.

[5] The DEFORM module has existed in some form (DEFORM-II, DEFORM-III) within the code since SAS2A, but DEFORM-4 and DEFORM-5 represent the latest accepted versions.

SAS4A/SASSYS-1 output to these experiments is not known to exist and would need to be recreated. Currently, several of these M-series tests are being utilized to validate the new DEFORM, PINACLE, and LEVITATE modules that will be released in a future SAS4A/SASSYS-1 version.

**Table 4.4: Summary of SAS4A/SASSYS-1 Legacy Validation**

| TREAT Test | Description | Version | Relevant Module(s) if Identified |
|---|---|---|---|
| R3, R4, R5 | FTR fuel pins ($UO_2$) in LOF | SAS3A | Boiling, CLAZAS |
| L5 | Mixed-oxide fuel in TUCOP | SAS3A | N/A |
| L6, L7, L8 | Mixed-oxide fuel in TUCOP | SAS3D | PRIMAR-3, SLUMPY |
| L6, L7, L8 | Mixed-oxide fuel in TUCOP | SAS4A | LEVITATE, PLUTO2, CLAP |
| H6, E8 | Mixed-oxide fuel in TOP | SAS4A | PLUTO2 |
| L03, L07 | Mixed-oxide fuel in TOP (L03) or TUCOP (L07) | SAS4A | PRIMAR4, DEFORM-4, PLUTO2, PINACLE, LEVITATE |
| TS-1, TS-2 | Mixed-oxide fuel in TOP | SAS4A | PINACLE, LEVITATE |
| M2, M3, M4, M7 | U-Fs, U-Pu-Zr (M7), U-Zr (M7) fuel in TOP | SAS4A | DEFORM-5, PINACLE, LEVITATE |
| M5, M6, M7 | U-Pu-Zr (M5, M6, M7) or U-Zr (M7) fuel in TOP | SAS4A | FPIN2 |
| RFT-L1 (HEDL) | Mixed-oxide fuel in TOP | SAS4A | N/A |

### *4.3.3 Benchmark Activities*

Numerous system-level benchmark analyses have been or are in the process of being completed using SAS4A/SASSYS-1. Completed integral assessments include the EBR-II Shutdown Heat Removal Tests (SHRT) [28] and the Phénix Natural Circulation (NC) Test [29], both of which were an International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP). Ongoing benchmark activities include analyses of the FFTF loss of flow without scram (LOFWOS) test, the Phénix Dissymmetric Test, and the Monju Turbine Trip Benchmark Problem. It should be noted that the latter two benchmark activities employ system-CFD analysis techniques.

The EBR-II SHRT benchmark activity focused on analysis of the SHRT-17 and SHRT-45R tests, which were protected and unprotected (respectively) full power loss of flow transients. The objective of SHRT-17 was to demonstrate the effectiveness of natural circulation in the reactor, while the objective of SHRT-45R was to demonstrate the ability of passive reactivity feedback to reduce the reactor to decay heat power levels. As such, key phenomena exhibited during these tests include flow coastdown behavior, development of natural circulation flow regimes, thermal stratification in pool volumes and the Z-pipe, and inherent reactivity feedback mechanisms (primarily fuel/core expansion, Doppler, and coolant feedback effects). Beyond the CRP activity, other unprotected loss of flow and loss of heat sink tests in the SHRT series have also been analyzed using SAS4A/SASSYS-1 and are documented in internal reports. This includes SHRT-45, which had identical experimental conditions as SHRT-45R; SHRT-43R, a loss of flow initiated at full flow and 70% power; BOP-301, a loss of heat sink at full flow and half power; and BOP-302R, a loss of heat sink at full flow and full power.

The Phénix NC Benchmark Test, conducted as part of the End of Life Test Campaign, examined a protected loss of heat sink transient from 35% power and 70% flow conditions with the objective of demonstrating the effectiveness of natural circulation in the primary system and the effect of dynamic heat rejection via secondary cooling systems. Approximately three hours following pump trips in the primary and secondary systems, heat rejection of the total system is augmented by air cooling of the steam generators, the effect of which is evident in primary and secondary system temperature conditions. Similar to the loss of flow tests in EBR-II, key phenomena exhibited during these tests include flow coastdown behavior, development of natural circulation flow regimes, and thermal stratification in pool volumes. Beyond the EBR-II SHRT benchmark tests, the NC test also introduces the effects of dynamic heat rejection during the transient.

As part of the upcoming IAEA CRP benchmark activity on the FFTF Passive Safety Test program, SAS4A/SASSYS-1 will be utilized to model Test #13, an unprotected loss of flow test from 50% power and 100% flow with the objective of demonstrating the effectiveness of passive reactivity feedback mechanisms and systems in reducing core power to decay heat levels. Two unique features were considered as part of this test: the gas expansion modules (GEMs), a passive system that inserted negative reactivity during reduced flow conditions, and a limited free bow core restraint system that enabled complex radial expansion in the core region. Key phenomena exhibited during this test include flow coastdown behavior, development of natural circulation flow regimes, effects inherent reactivity feedback mechanisms, and the effects of passive reactivity insertion mechanisms. Preliminary results of SAS4A/SASSYS-1 analyses can be found in [30].

Another component of the Phénix End of Life Test Campaign, the Dissymmetric Test examined a protected loss of heat sink from full power and full flow conditions in the Phénix reactor. As heat rejection and flow in the secondary systems were not reduced simultaneously in the test, the objective of the exercise was to examine the effect asymmetric heat rejection conditions via the intermediate heat exchangers on primary system dynamics, particularly in the short term, while the primary system maintained full flow conditions. System-level 0-D and 1-D codes cannot capture asymmetric conditions in pool volumes, meaning coupling with CFD codes is required for effective analysis. Under an International Nuclear Energy Research Initiative (INERI) collaboration with the European Union, SAS4A/SASSYS-1 coupled with STAR-CCM+ is being utilized to complete the benchmark activity, which has recently entered the open phase [31]. On the European side, this effort is supported as part of a larger Horizon 2020 project titled “Thermal-Hydraulics Simulations and Experiments for the Safety Assessment of Metal Cooled Reactors (SESAME)”. Key phenomenon exhibited during this test include the development of complex flow regimes in primary system pools at full flow conditions due to asymmetric heat rejection.

The Monju Turbine Trip Benchmark Problem examines a protected loss of heat sink from 40% power and full flow conditions, with the objective of examining the effects of natural circulation and thermal stratification in the upper plenum region. Given the objectives to examine multidimensional effects, coupling of a system-level code to CFD is required. Therefore, like the Dissymmetric Test, this exercise also utilizes SAS4A/SASSYS-1 coupled to STAR-CCM+. The activity, a part of the ongoing Civil Nuclear Working Group (CNWG) bilateral agreement between Japan and the U.S., is expected to conclude in the near-term. Key phenomena exhibited during this test include flow coastdown behavior, the development of natural circulation flow regimes, and pool stratification.

### *4.3.4 Development and Qualification of Mechanistic Fuel Performance Models*

To simulate postulated Unprotected Loss-of-Flow accident scenarios, the metallic fuel models and severe accident analysis capabilities of SAS4A/SASSYS-1 have been improved. In-pin plenum fission gas and sodium release upon clad failure and in-pin fuel freezing are the major modeling activities that have been completed. Additionally, other modeling and numerical improvements have been accomplished to improve the predictions of SAS4A/SASSYS-1 with respect to pre-transient fuel performance model, transient fuel performance model, in-pin molten fuel motion model, and post-failure fuel relocation model.

Benchmarking of the developmental version of the code using EBR-II, FFTF, Phénix pre-transient data, TREAT transient overpower tests, and separate effect tests has been performed. However, these benchmark evaluations have been performed in a limited capacity that does not adhere to the guidance in Section 2.4. These new EM capabilities are currently undergoing extensive verification and validation that complies with the guidance in Section 2.4. These models are considered relevant to both single- and multiple-fault events as they enable improved predictive capabilities of the margins preceding the severe accident domain (e.g. fuel/clad failure margins).

### *4.3.5 Phenomena, Benchmarks, and Validation Test Matrix*

The adequacy of the SAS4A/SASSYS-1 intrinsic models can be assessed using experimental data originating from a combination of SETs and IETs. These cases have been chosen to cover the most important basic models and correlations in SAS4A/SASSYS-1 based on available experimental data. Table 4.5 provides a brief summary of the current status of validation test problem availability [32, 33]. However, it should be noted that documentation supporting these tests does not comply with the guidance outlined in Section 2.4.

**Table 4.5: Model Validation Test Matrix**

| | EBR-II | FFTF | Phénix | TREAT | SETs |
|---|---|---|---|---|---|
| **Basic Phenomenological Models** | | | | | |
| Frictional pressure losses | X | X | X | | |
| Wall surface roughness | X | X | X | | |
| Wall drag friction | X | X | X | | |
| Orifice losses | X | X | X | | |
| Gravity-head term | X | X | X | | |
| Fuel radial heat conduction | X | | X | | |
| Fluid axial heat conduction | | | X | | |
| Convection heat transfer | X | X | X | | |
| Fuel (fuel/gap/clad) models | X | X | | | |
| Adiabatic inner surface | X | X | X | | |
| Materials properties data | X | X | X | | |
| Parallel channel flow | X | X | X | | |
| Plenum coupling | X | X | X | | |
| Wall heat transfer for components | | | X | | |
| Reactivity feedback | | X | | | |
| Wire spacer friction | X | X | | | |
| Momentum convection | | | X | | |
| Subchannel mixing | | | X | | |
| **Boundary Conditions** | | | | | |
| Mass flow function/table BC | | X | | | |
| Inlet/Outlet pressure function/table BC | | | | | |
| Inlet temperature function/table BC | | X | | | |
| Power vs time | X | X | X | | |
| **Types of Calculations** | | | | | |
| Single-phase flow transient | X | X | X | | |
| Transient heatup/cooldown | X | X | X | | |
| Pump coast-down | X | | X | | |
| Thermal stratification | X | | X | | |
| Transition to natural circulation | X | X | X | | |
| Core flow redistribution | X | X | X | | |
| Subassembly flow redistribution | | | | | |
| Numerical convergence | | | | | |
| Restart calculation | X | | | | |
| Calculation reproducibility | X | | | | |
| All control signal parameters | | | X | | |
| **Components** | | | | | |
| Pipe | X | X | X | | |
| IHX – Tube Side | X | X | X | | |
| IHX – Shell Side | X | X | X | | |
| Core Channel | X | X | X | | |
| Bypass Channel | X | | | | |
| Pump impeller | X | X | X | | |
| Annular Element | | | X | | |
| Check Valve | | | | | |
| Inlet Plenum | X | X | X | | |
| Outlet Plenum, No Cover Gas | | | | | |
| Outlet Plenum, Cover Gas | X | X | X | | |
| Incompressible Liquid, No Gas | | | | | |
| Pool, Cover Gas | X | X | X | | |
| Gas Volume | | | | | |
| Electromagnetic Pump | | | | | |

| | EBR-II | FFTF | Phénix | TREAT | SETs |
|---|---|---|---|---|---|
| Centrifugal Pump | | | | | |
| Homologous Pump | X | X | X | | |
| EBR-II Pump | | | | | |
| Pump Head/Time Table | | | | | |
| Pump Speed/Time Table | X | X | X | | |
| Pump Torque/Time Table | | | X | | |
| **Metallic Fuel Models** | | | | | |
| Clad Strain | X | X | | | |
| Clad Wastage | X | | | | X |
| Fission Gas Release | X | X | X | | |
| Fuel Axial Elongation | X | X | X | | |
| Fuel Constituent Redistribution | X | | | | |
| Reactivity Worth | | | | X | |
| Iron Bearing Layer Formation | | | | | |
| Eutectic Penetration | | | | | X |
| Cladding Failure | | | | X | X |
| Sodium Length in Upper Plenum | | | X | | |

### *4.4 Documentation*

Documentation on the models contained within and usage of SAS4A/SASSYS-1 exists primarily in the form of a code manual. Some internal memos describing model designs or solution methodologies are known to exist, but many of these materials are likely to be outdated or scoped by the code manual. The most recent SAS4A/SASSYS-1 manual, released in 2017 for v5.0 [1], is largely derived from documentation developed in 1996 for v3.0 [34]. Despite the 20-year gap in documentation release, material developed in support of v3.0 does apply to v5.0, and an effort to address outdated or incorrect information (primarily related to usage) in the 2017 release has been completed for all models utilized to assess design basis events.

The manual, which consists of approximately 2000 pages, provides descriptions of the equations, discretization, and solution methods used, where the level of detail varies per model. Considering the requirements of modern SQA frameworks, SAS4A/SASSYS-1 documentation is significantly lacking in the areas of requirement specification and design implementation as it relates to software architecture. However, software design is well-addressed with respect to theory for most models in the code, with model descriptions provided on a per-module basis. User inputs are also well described, with some inputs including the corresponding recommended values. However, there is limited to no documentation regarding the valid range of models, inputs, correlations, etc. Selected chapters of the manual that relate to phenomena typically included in the design basis space and a brief description of each chapter are listed in Table 4.6.

Documentation pertaining to the current V&V status of the code is limited. Documentation on the V&V Test Suite described in Section 4.3.1 is limited to internal Argonne reports, but it does address requirements, testing, and acceptance criteria for the various tests. As discussed in Section 4.3.2, the majority of historical validation efforts and supporting documentation either has limited relevance to the current code or simply does not comply with modern V&V/SQA requirements. Documentation on the benchmark activities described in Sections 4.3.3, 4.3.4, and 4.3.5 is either currently available or will be available upon public release of compiled benchmark reports. It is expected that the level of detail available in benchmark reports (available both internally and publicly) would be sufficient to support software qualification to the extent that they describe code behavior and results for specific models and transient phenomena, however they will largely lack documentation of valid input and model ranges.

**Table 4.6: Selected Contents of SAS4A/SASSYS-1 Manual**

| Chapter | Description |
|---|---|
| User Guide | Provides descriptions of user inputs for all locations, high-level software architecture, solution methodologies, and some example problems. |
| Steady State and Transient Thermal Hydraulics in Core Channels | Provides descriptions of core channel modeling approach, pin meshing, assembly nodalization/zoning, steady-state and transient solution methodologies, subassembly-to-subassembly heat transfer, fuel-cladding-coolant heat transfer, the multiple-pin and subchannel models, and module-specific user input and program flow. |
| Reactor Point Kinetics, Decay Heat, and Reactivity Feedback | Provides descriptions of the solution methods for decay heat, point kinetics, reactivity feedback (per mechanism) calculations, and module-specific user input and program flow. |
| Primary and Intermediate Loop Thermal Hydraulics | Provides descriptions of steady-state and transient solution methods for hydraulics and temperatures in ex-core heat transport systems, including components (e.g. compressible volumes, elements, pumps, etc.), time stepping schemes, and module-specific user input and program flow. |
| Control System | Provides descriptions the generalized control system model, steady-state and transient solution methods, block/signal functionality, and user implementation. |
| Balance of Plant Thermal/Hydraulic Models | Provides descriptions of the analytical and discretized solution methods, plant nodalization user implementation, steady-state and transient solution algorithms, component (e.g. steam drum, condenser, reheater, etc.) solution methodologies, and user input. |
| SSCOMP: Pre-Transient Characterization of Metallic Fuel Pins | Provides descriptions of solution methods for key metallic fuel pin phenomena that occur during steady-state irradiation (e.g. fuel/clad expansion, fuel constituent and bond sodium migration, etc.), including key correlations, and user input. |
| Sodium Voiding | Provides descriptions of two-phase coolant modeling methodology, time stepping schemes, program flow, and user input. |

# 5 Qualification Support Gap Analysis

This section provides a gap analysis regarding the documentation required to support use of SAS4A/SASSYS-1 in a license application. Given the overview of qualification and dedication requirements provided in Section 2, these gaps have been characterized into two categories: verification as it relates to the SAS4A/SASSYS-1 SQA Program (Section 5.1), and validation as it relates to model qualification (Section 5.2).

## *5.1 Verification Gaps*

While the existing SAS4A/SASSYS-1 SQA Program ensures compliance with most SQA best practices and requirements found in [2, 3] for *new* software development activities, the majority of SAS4A/SASSYS-1 development predates the establishment of modern SQA practices. Therefore, it is expected that some level of effort will be required to establish some elements of standard software verification documentation than can support qualification of legacy components of the code.

Table 5.1, partially derived from [35], provides an overview of the existing SAS4A/SASSYS-1 verification gaps as they relate to software qualification and dedication. Additional details on these gaps can be found below. It should be noted that closure of these gaps will directly support closure of the gaps identified in Section 5.2.

**Table 5.1: Prioritized SAS4A/SASSYS-1 Verification Gaps**

| Gap | Importance | Lead Time | Comment |
|---|---|---|---|
| Software Requirements Specification per component | Medium | Long | Limited requirements documentation available. |
| Software Design Description per component | High | Medium | Code Manual [1] provides fairly comprehensive design description, however limited documentation of model applicability and input limitations is available. |
| Verification Testing per component | Medium | Medium | Partially addressed by existing V&V Test Suite. Needs to be resolved on case-by-case basis. |
| V&V Test Suite (Section 4.3.1) | Medium | Ongoing | Test suite improvement expected to occur throughout lifetime of project. |

Generation of requirements, design, and testing documentation is an essential component of software verification. Software requirements specifications (SRS) are intended to comprehensively describe the functional and performance requirements (e.g. the code must model a core with hexcan geometry, or the code must complete the simulation in approximately real-time) of the models that are to be developed. In the case of SAS4A/SASSYS-1, very limited documentation describing software requirements is available, largely due to the legacy R&D environment in which it was developed. Software Design Descriptions (SDD) provide information on the design and implementation of the model, including the design data structures, architectures, interfaces, etc., and the applicability ranges of models and inputs. The SAS4A/SASSYS-1 Code Manual satisfies most requirements of an SDD, as the Manual provides fairly comprehensive descriptions of the phenomenological models implemented in the code. Despite the large volume of information available in the Code Manual, significant gaps in the design description of SAS4A/SASSYS-1 still exist (e.g. documentation of acceptable input ranges for critical characteristics, updated documentation of code architecture, etc.). Lastly, verification testing is also required on a per component basis to demonstrate that each module or feature complies with stated requirements and that the design is implemented appropriately. The V&V Test Suite (Section 4.3.1) supports this to some degree, but some gaps do remain.

Regarding the V&V Test Suite, addition of test problems is expected to occur throughout the lifetime of the software project as new models and features are implemented, as this is a requirement of the SQA Program. Integration of standardized problems supports acceptance testing requirements as they relate to verification of software requirements conformance and design implementation for new models as well as regression testing of legacy models.

## *5.2 Validation Gaps*

While the SAS4A/SASSYS-1 SQA Program is designed to formally address software verification, there currently exists no formal process to manage software validation. As such, a listing of validation gaps has been developed in Table 5.2 as they relate to software qualification. These gaps have been derived from the summary requirements identified in Section 2.4. This table also denotes relevance of the gap to existing SQA Program components, as these documentation gaps should be addressed in accordance with Program requirements. Furthermore, it is expected that materials supporting closure of these gaps will be integrated into SQA Program documentation that supports code pedigree. Additional discussion of these gaps is provided below.

**Table 5.2: Qualification Gaps**

| Gap | Comment | Relevant SQA Program Component |
|---|---|---|
| SET/IET Validation | Code qualification reports describing the qualification of the EM against separate effects test data, integral system effects tests and plant data are needed. | N/A |
| Valid Numerical Model Bounds | Code qualification reports are needed which detail the range of applicability of the important basic models and correlations based on separate effect tests and sensitivity analyses. Results and associated uncertainties applicable to such models need to be incorporated into the qualification documentation. | SRS, SDD, V&V Test Suite |
| Valid Input Bounds | Code Manual and EM qualification documentation is needed to detail the acceptable input value bounds. These bounds can be based on EM uncertainty quantification and sensitivity analyses. | SRS, SDD, V&V Test Suite |
| Default/Suggested Inputs | Code manual and EM qualification documentation is needed to detail default or suggested input values where the latter is not available to the code user. These values can be based on EM uncertainty quantification and sensitivity analyses. | SRS, SDD |

As indicated in Table 5.2, demonstration of the SAS4A/SASSYS-1 numerical model validity and characterization of model applicability range is incumbent upon the determination of the experimental and numerical uncertainties associated with the SET/IET benchmark cases. Simulation uncertainties are generally determined based on geometric and modeling parameters, material properties, and modeling assumptions. In order to assess the effects of the uncertainties and determine the safety margins for a specific reactor design, uncertainty quantification (UQ) and sensitivity analysis are required.

Quantifying these experimental uncertainties is paramount to determining the EM inherent numerical error. Sensitivity analyses, on the other hand, are important to explore the sources of variability in computational results. For code validation, the experimental uncertainty, which is composed of measurement, material, and geometry uncertainties (i.e., due to the inherent experimental uncertainty in measurements and due to the manufacturing tolerances for any given structural component), needs to be known.

SAS4A/SASSYS-1 numerical model and correlation uncertainty is likely to be best characterized for smaller, focused experiments such as SETs. Experimental uncertainties shall be provided by the owners of the experiment data. SAS4A/SASSYS-1 EM overall uncertainty is likely to be best quantified through qualification analyses of larger experiments, such as IETs, where interactions between the various components in the system are studied.

Uncertainty quantification is an ongoing effort and individual uncertainty characterization has been explored for SAS4A/SASSYS-1 [36]. This effort, however, is reduced in scope. The code validation process aims at identifying the constituents of the EM uncertainty such as experimental and numerical correlation uncertainties on a larger scale to be able to characterize SAS4A/SASSYS-1 EM overall uncertainty.

# 6 Summary and Path Forward

As discussed in Section 2, a commercial applicant is expected to align with the software qualification and commercial grade dedication requirements for any safety analysis within a license application. Acceptance of the code during qualification/dedication typically includes review of both the verification and validation properties of the software. To improve the regulatory acceptability of the SAS4A/SASSYS-1 advanced reactor safety analysis system software, a software qualification and dedication gap analysis as it relates to code documentation has been performed. This effort leverages the expertise and framework established as part of the SAS4A/SASSYS-1 SQA Program.

A high-level review of typical SFR transient phenomena has been completed for a standardized plant that broadly represents domestic vendor designs. A listing of cross-cutting phenomena for which software qualification activities will be required was developed in Table 3.6. Simplistically, cross-cutting areas were identified to include the items identified in Table 6.1.

**Table 6.1: High-Level Cross-Cutting Phenomena**

| High-Level Cross-Cutting Phenomena |
|---|
| *Reactivity feedback response prior to scram* |
| *System-wide thermal inertia (structures, components, coolant)* |
| *Transition in natural circulation flow regime in heat removal systems* |
| *Decay heat generation* |
| *Steady-state fuel characterization* |
| *Clad/fuel behavior at elevated temperatures* |
| *Point kinetics and decay heat* |
| *Pump coastdown behavior* |
| *Core flow redistribution in loss of forced convection* |
| *Pool stratification* |

Based on the findings outlined in Section 5, a path forward for continued pedigree improvements has been developed in Table 6.2. These gaps should be resolved on a prioritized basis, beginning with the functional capabilities identified in Table 6.1. Prioritized gaps include the need for documentation of the bounds of internal numerical models and user inputs. Development of this documentation should be an integral component of the SQA Program, and can be accomplished via a staged approach in which software design documentation is gradually improved on a prioritized basis. These items are expected to have a medium lead time to achieve a comprehensive documentation status, but significant progress on key phenomena can be achieved in the near-term.

**Table 6.2: Prioritized Qualification Gaps**

| Gap | Importance | Lead Time | Comment |
|---|---|---|---|
| Valid Numerical Model Bounds | High | Medium | Can be completed for high-priority models in short term, but comprehensive documentation requires medium lead time. This is supported by SQA Program activities. |
| Valid Input Bounds | High | Medium | Can be completed for high-priority models in short term, but comprehensive documentation requires medium lead time. This is supported by SQA Program activities. |
| Validation Matrices | Medium | Short | Additional review of existing test problems is required to characterize relevant detailed phenomena. |
| SET/IET Validation | Medium | Long | Should be completed on prioritized basis as per findings of mature validation matrices and review in Section 3.2. |
| SA/UQ | Medium | Long | Supports identification of inherent numerical errors. Requires very long lead time for comprehensive, effective studies. |
| Default/Suggested Inputs | Low | Medium | Can be completed in part in conjunction with identification of valid input bounds. This is supported by SQA Program activities. |

Improvements to the validation matrix in Section 4.3.5, completion of SET/IET validation, and completion of sensitivity analysis and uncertainty quantification studies for key phenomena are identified as having a medium priority with varying lead times. The former two items directly support software validation, whereas the latter augments both software design and validation. Development of an improved validation matrix will help to identify gaps in the availability of SET and IET problems.

An important step in validation is the development of more comprehensive validation matrices for both code development and code validation. A listing of test suite cases and legacy code validation has been prepared in Table 4.5. Numerous system-level benchmark analyses have been or are in the process of being completed using SAS4A/SASSYS-1. Completed integral assessments include the EBR-II Shutdown Heat Removal Tests (SHRT) and the Phénix Natural Circulation Test. Ongoing benchmark activities include analyses of the FFTF loss of flow without scram (LOFWOS) test, the Phénix Dissymmetric Test, and the Monju Turbine Trip Benchmark Problem. However, these validations do not rigorously identify the specific phenomena that need to be validated within the qualification and commercial grade dedication framework. As such, additional effort is needed to generate a matrix of separate, mixed and integral effect experiments spanning the anticipated length and time scales as well as to document the identified critical characteristics and EM acceptance criteria for code qualification.

Extensive sensitivity analysis and uncertainty quantification (SA/UQ) must be performed to characterize the inherent variability of SAS4A/SASSYS-1 computational results. This item is identified have a medium priority with a long lead time due to the broad range of applicable

SA/UQ studies. The code validation process aims at identifying the constituents of the EM uncertainty such as experimental and numerical correlation uncertainties. Experimental uncertainties are incumbent upon measurement, material and geometry uncertainty characterization. These constituents ultimately compose the inherent experimental measurement uncertainty and manufacturing tolerances for any given structural component. Quantifying these experimental uncertainties are paramount to determine the EM inherent numerical error. SAS4A/SASSYS-1 numerical model and correlation uncertainty is likely to be best characterized for smaller, more focused experiments such as SETs. Experimental uncertainties shall be provided by the owners of the experiment data. SAS4A/SASSYS-1 EM overall uncertainty is likely to be best quantified through qualification analyses of larger experiments, such as IETs, where interactions between the various components in the system are studied.

Lastly, software design documentation and the Code Manual should be updated to include specification of default or suggested inputs. This assists with usability of the software and constituent model qualification, but is identified as having a relatively low priority. This activity can be in part completed in conjunction with identification of valid input bounds.

# References


[1] T. H. Fanning, A. J. Brunett, and T. Sumner, eds., "The SAS4A/SASSYS-1 Safety Analysis Code System: User's Guide," Argonne National Laboratory, ANL/NE-16/19, 2017.

[2] American Society of Mechanical Engineers, "Quality Assurance Requirements for Nuclear Facility Applications," ASME NQA-1-2008, 2008.

[3] American Society of Mechanical Engineers, "Addenda to ASME NQA-1-2008: Quality Assurance Requirements for Nuclear Facility Applications," NQA-1a-2009, 2009.

[4] U.S. Nuclear Regulatory Commission, "Transient and Accident Analysis Methods," Regulatory Guide 1.203, 2005.

[5] U.S. Nuclear Regulatory Commission, "Quality Assurance Program Criteria (Design and Construction)," Regulatory Guide 1.28, Rev. 4, 2010.

[6] Electric Power Research Institute, "Plant Engineering: Guideline for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications: Revision 1 of 1025243," EPRI TR 3002002289, 2013.

[7] U.S. Nuclear Regulatory Commission, "Report to Congress: Advanced Reactor Licensing," 2012.

[8] M. Denman, J. LaChance, T. Sofu*, et al.*, "Sodium Fast Reactor Safety and Licensing Research Plan - Volume I," SAND2012-4260, 2012.

[9] U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," NUREG-0800, 2007.

[10] J. C. Carter et al., "SAS1A, A Computer Code for the Analysis of Fast-Reactor Power and Flow Transients," Argonne National Laboratory, ANL-7607, 1970.

[11] F. E. Dunn et al., "The SAS2A LMFBR Accident-Analysis Computer Code," Argonne National Laboratory, ANL-8138, 1974.

[12] M. G. Stevenson et al., "Current Status and Experimental Basis of the SAS LMFBR Accident Analysis Code System," in *Proceedings of the Fast Reactor Safety Meeting*, Beverly Hills, CA, 1974, pp. 1303-1321.

[13] F. E. Dunn, "Code Portability and Data Management Considerations in the SAS3D LMFBR Accident-Analysis Code," presented at the National Computer Conference, Chicago, IL, 1981.

[14] G. Birgersson et al., "The SAS4A LMFBR Accident Analysis Code System," Argonne National Laboratory, ANL/RAS-83-38, Rev. 2, Vol. 1 and 2, 1988.

[15] A. M. Tentner and Kalimullah, "SAS4A Analysis of the M7 Metal Fuel Treat Experiment," Argonne National Laboratory, ANL-IFR-186, 1993.

[16] F. E. Dunn et al., "The SASSYS-1 LMFBR Systems Analysis Code," Argonne National Laboratory, ANL/RAS-84-14, Rev. 1, 1987.

[17] C. E. Till, "Fast Reactor Directions: The LMR Integral Fast Reactor Program at Argonne," in *Proceedings of the International Fast Reactor Safety Meeting*, Snowbird, UT, 1990.

[18] Argonne National Laboratory, "The SAS4A/SASSYS-1 LMR Analysis Code System, Vol. 1-5," ANL-FRA-1996-3, 1996.

[19] J. Sackett et al., "EBR-II Test Programs," in *Proceedings of the International Fast Reactor Safety Meeting*, Snowbird, UT, 1990.
[20] T. H. Fanning, ed., "The SAS4A/SASSYS-1 Safety Analysis Code System: User's Guide," Argonne National Laboratory, ANL/NE-12/4, 2012.
[21] A. J. Brunett and L. L. Briggs, Unpublished Information, 2015.
[22] U.S. Department of Energy, "Quality Assurance," DOE O 414.1D, 2011.
[23] U.S. Department of Energy, "Safety Software Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance," DOE G 414.1-4, 2005.
[24] Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Quality Assurance Plans," Software Engineering Standards Committee of the IEEE Computer Society, IEEE Std 730-2002, 2002.
[25] B. Collins-Sussman, B. W. Fitzpatrick, and C. M. Pilato, "Version Control with Subversion," http://svnbook.red-bean.com, 2017.
[26] Edgewall Software, "Trac: Integrated SCM & Project Management," https://trac.edgewall.org, 2017.
[27] Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Conifguration Management Plans," Software Engineering Standards Committee of the IEEE Computer Society, IEEE Std 828-2005, 2005.
[28] International Atomic Energy Agency, "Benchmark Analysis of EBR-II Shutdown Heat Removal Tests," IAEA-TECDOC-1819, 2017.
[29] International Atomic Energy Agency, "Benchmark Analyses on the Natural Circulation Test Performed During the PHENIX End-of-Life Experiments," IAEA TECDOC 1703, 2013.
[30] G. Zhang, A. Moisseytsev, T. Sumner*, et al.*, "Preliminary Analysis of FFTF Loss-of-Flow Tests with SAS4A/SASSYS-1," in *Proceedings of the 2017 ANS Annual Meeting*, San Francisco, CA, 2017.
[31] B. Grosjean and C. Geffray, unpublished information, French Alternative Energies and Atomic Energy Commission (CEA), 2018.
[32] R. Hu, "Verification and Validation Plan for the SFR System Analysis Module," Argonne National Laboratory, ANL/NE-14/14, 2014.
[33] A. Tentner and A. Karahan, "Unpublished information," Argonne National Laboratory2018.
[34] Reactor Analysis Division, "The SAS4A/SASSYS-1 LMR Analysis Code System," Argonne National Laboratory1996.
[35] A. J. Brunett, L. L. Briggs, and T. H. Fanning, "Status of SFR Codes and Methods QA Implementation," Argonne National Laboratory, ANL-ART-83, 2017.
[36] G. Zhang, T. Sumner, and T. Fanning, "Uncertainty Quantification of EBR-II Loss of Heat Sink Simulations with SAS4A/SASSYS-1 and Dakota," in *International Conference on Fast Reactors and Related Fuel Cycles: Next Generation Nuclear Systems for Sustainable Development (FR17)*, Yekaterinburg, Russian Federation, 26-29 June 2017.

# Appendix A

**Table A.1: Product Selection Attributes [6]**

| Product Selection Attribute | Description | Acceptance Criteria | Possible Evaluation Method |
|---|---|---|---|
| Functionality required for intended end-use: the program is capable of performing the desired calculations, analyses, etc. | When correctly installed in the designated environment, the program is capable of performing the types of calculations required over the identified range of inputs. | The program includes the capabilities specified/necessary. *Note:* Verification of the capabilities for acceptance occurs after product design, selection, and establishment of suitability for use are complete. | Review of available product literature. |
| Validity of scientific basis for computer program functionality: The computer program basis is consistent with the appropriate engineering scientific research and technical approaches. | The degree to which the computer program's results correlate with experimental data, expected data results, or professional analyses and the degree to which any erroneous data sets do not correlate with experimental data or professional analyses. | Consistency with research and professional technical approaches is based upon peer-reviewed published technical papers or industry-accepted computer programs performing a similar function. The output of the program can be viewed as how closely the computer program's output matches technical reports or baseline (industry accepted) program output. | Engineering and/or subject matter expert review of documentation associated with the program. Evaluation may include:<br>• Comparison of technical publication results against the program's output for a similar problem.<br>• Comparison of the baseline program output against the program's output that is being dedicated. Both programs must solve the same or closely similar physical problem.<br>• A review of the program's current user base and its applicability to the intended use. |
| Effective problem reporting. | An institutionalized process used by the supplier to both receive problem reports and provide user notification of potential errors/limitations, patches, updates, etc. | A formal, documented problem reporting program exists and is effectively implemented. A documented process exists to track customers and provide notification when appropriate. Evaluation criteria for determining when notifications are warranted are documented and include appropriate thresholds. Problem reporting | Verification is performed by a review of communications regarding errors with users, a review of any form of communication with the supplier, and a review of a communications log. |

| Product Selection Attribute | Description | Acceptance Criteria | Possible Evaluation Method |
|---|---|---|---|
| | | metrics are maintained and indicate an appropriate number of notifications to users over time. | |
| Supportability/maintainability | The ability of the supplier to continue providing support for the program over the life of its use. | Standard financial models used to evaluate suppliers; stability of the supplier/business longevity; size of customer base; plans for future product updates/releases; supplier's history of discontinuing products. | Review of the supplier history for the specific computer program as well as the history in supporting similar computer programs or products. |
| Supportability/maintainability | *If applicable:* The program is designed in a way that permits modification to be performed. | Time and skills required to modify the program. | Review of supplier metrics associated with length of time to evaluate, implement, and test a change/error correction, update all documentation, and release the change. |
| Environment compatibility: portability | The measure of the effort required to migrate the computer program to a different platform, component, or environment. *Note:* this attribute only relevant if migration is anticipated. | As described in software requirements. | Performing migration to one or more environments equivalent to the dedicating entities. |

**Table A.2: Product Identification Attributes [6]**

| Inspection Attribute | Description | Acceptance Criteria | Possible Verification Method During Receipt |
|---|---|---|---|
| Host system and/or environment identification | Information that identifies the host system(s) or operating environment(s) suitable for execution of the program. | Identifying information matches the host computer system(s) or environment(s) included in the applicable specification or procurement document. | Review of product identification and documentation during receipt inspection. |
| Computer program identification | Complete information required to identify base computer program, build number, version number, included patches, etc. | Computer program identification matches the criteria specified in the specification/procurement document. | Review of product identification and documentation during receipt inspection. |

**Table A.3: Performance Critical Characteristics [6]**

| **Performance Critical Characteristic** | **Description** | **Acceptance Criteria** | **Possible Verification Method** |
|---|---|---|---|
| Accuracy of output | The degree to which there is a close correlation with the expected or desired outcome. | Objective evidence through testing or similar means that the program results meet the user's specified requirements (e.g. Accuracy - ± *x*%). | Inspection and testing (Method 1); commercial-grade survey of testing activities and documentation; observation and review of design (Method 3); review of the installed base to determine performance history (Method 4). |
| Precision of output | The degree of repeatability or degree of measure. | Objective evidence through testing or similar means that the program results meet the user's specified requirements (e.g. Precision - ± 0.000*x*). | Inspection and testing (Method 1); commercial-grade survey of testing activities and documentation; observation and review of design (Method 3); review of the installed base to determine performance history (Method 4). |
| Tolerance of output | The allowable possible error in measurement. | Objective evidence through testing or similar means that the program results meet the user's specified requirements (e.g. Tolerance - ± 0.000*x*). | Inspection and testing (Method 1); commercial-grade survey of testing activities and documentation; observation and review of design (Method 3); review of the installed base to determine performance history (Method 4). |
| Functionality: Specific safety functions and algorithms | Critical functions or calculations are performed. For example, time-dependent functions and functionality to allow only authorized users access to perform the safety-related calculations. | As described in program requirements or procurement documentation. | Inspection and testing (Method 1); observation and review of design (Method 2 and/or 3); review of the installed base to determine performance history (Method 4). |
| Functionality: Completeness and correctness | The degree to which the program requirements, design, and implementation satisfy applicable requirements. Formal techniques may be used to mathematically prove that the computer program satisfies its specified requirements. This critical characteristic helps to identify the | Completeness and correctness are based upon how many of the program's requirements have been verified to be successfully implemented. | Performing a review of the functional requirements' traceability to test cases and verification that the test results indicate correct functionality. If the requirements' traceability is unavailable, the dedicating entity can develop the traceability matrix from the program's requirements or procurement specifications and test cases performed (Method 2). |

| Performance Critical Characteristic | Description | Acceptance Criteria | Possible Verification Method |
|---|---|---|---|
| | risks of the program failure to execute its safety functions. | | |
| Interfaces: Critical input parameters and valid ranges | The set of input parameters that are used in the critical functions of the program and range of their valid values. This critical characteristic ensures that the program will function properly for all possible ranges of operational inputs required. | As described in program requirements or procurement specification documentation. | Inspection and testing (Method 1); inspection of user's manual (Method 1); observation and review of design and/or implementation (Method 2 and/or 3); review of the installed base to determine performance history (Method 4). |
| Interfaces: Output parameters | The characteristics of the critical output parameters, including file formats and mathematical notations. This critical characteristic ensures that the program output is expressed in the required expected format or units. | As described in program requirements or procurement specification documentation. | Inspection and testing (Method 1); observation and review of design (Method 3); review of the installed base to determine performance history (Method 4). |

**Table A.4: Dependability Critical Characteristics [6]**

| Dependability Critical Characteristic | Description | Acceptance Criteria | Possible Verification Method |
|---|---|---|---|
| Built-in quality: effective quality and oversight of development process | The development process is performed in accordance with a documented, effective QA program, plan, and/or procedures. | Objective evidence that demonstrates: the computer program was developed in accordance with a documented quality assurance program that was effectively implemented throughout the development process; the quality assurance program includes measures to ensure that the computer program is capable of performing functions included in the | Method 2 – Commercial-grade survey with technical subject matter expert participation; Method 3 – Source surveillance with technical subject matter expert participation to examine documented quality program documents and records associated with the development process. Review of third-party certification/accreditation reports and documentation; Review of internal/external audit reports. |

| Dependability Critical Characteristic | Description | Acceptance Criteria | Possible Verification Method |
|---|---|---|---|
| | | requirements specifications and/or design documents; in the case of an accredited QA program, accreditation of the developing organization throughout the development process. | |
| Built-in quality: Structured development process; Documentation | Development process is structured and documented. The process is clearly designed to achieve the functionality specified and to meet the requirements that are defined and documented. | Objective evidence demonstrates that: the development process is documented in procedures or other types of work instructions; the process is designed to achieve the defined and documented functionality. | Commercial-grade survey with subject matter expert participation (Method 2); Source surveillance with a technical subject matter expert at key points in the development process and associated testing (Method 3). |
| Built-in quality: Structured development process; Adherence to coding practices | The computer program complies with applicable coding standards, or use of code libraries. Adherence to coding practices typically reduces the likelihood of unidentified errors in the computer program. | Coding practices can be expressed in terms of the amount of code developed independent of applicable coding practices or without the use of applicable code libraries. | Commercial-grade survey with subject matter experts (Method 2); Source surveillance with a technical subject matter expert at key points in development process and associated testing (Method 3). |
| Built-in quality: Structured development process; Configuration control and traceability | Changes in the program are controlled and documented; Changes are traceable to specific builds or versions so that users may be notified of problems; etc.; Changes are subject to acceptance testing commensurate with testing applied to the original code. | Configuration of the computer program is controlled by use of an automated configuration management tool or other effective method; The configuration of the computer program is controlled as well as alignment with and revision of associated software and documentation.; The ability to support incoming and outgoing problem reporting process is maintained. | Commercial-grade survey with subject matter experts (Method 2); Source surveillance with a technical subject matter expert at key points in development process and associated testing (Method 3). |

| Dependability Critical Characteristic | Description | Acceptance Criteria | Possible Verification Method |
|---|---|---|---|
| Built-in quality: Code structure (complexity, conciseness) | The degree to which the computer program is legible, the complexity is minimized, and the code length is minimized. This critical characteristic provides an indicator of the difficulty to perform verification reviews and testing. | Code structure criteria can be quantitative (use of static analysis tools) or qualitative (reviews of the documented design or inspection of the code). Examples include: number of internal subroutine interfaces, number of do-loops, number of exits from a module, flow of logic, module depth/breadth, etc. | Review of supplier-documented evidence from the use of a static analysis tool or the dedicating entity performing an inspection and manual analysis of the documented design or code (Method 2). |
| Built-in quality: Conformance to national codes, standards, and industry-accepted certifications | The computer program's compliance with applicable national codes and standards or industry-accepted certifications. | Conformance criterion can be a measure of how well the program meets industry-accepted practices that provide a qualitative pedigree of the program. The criteria can be the degree to which a national code, standard, or certification program is achieved (e.g. 90% compliance with a specific standard). | Inspection of supplied-performed assessments of the computer program against the national code or standard (Method 1). Inspection of the proof of third-party certification (Method 1); Review of computer program documentation against the selected national code or standard (Method 2). |
| Built-in quality: Internal reviews and verifications | Effective use of analysis methods during development of the program to confirm compliance with requirements and identify errors and noncompliance with supplier procedures and standards. | Criteria for internal reviews and effectiveness of verifications are based upon the ratio of errors identified during review/verification and the number of errors discovered in the next life cycle phase. | Inspection and analysis of results from reviews or verification and validation activities performed in two or more adjacent life cycle phases (Method 2 and/or Method 3). |
| Built-in quality: Testability and thoroughness of testing | A measure of the completeness of the computer program verification, validation, and installation testing to ensure that the computer program is correct and complete. This critical characteristic may be appropriate for | Testability criteria are based on the ease or difficulty in conducting verification and validation activities as well as the scope of testing being performed. Testability criteria may include: the number of hours needed to perform peer reviews, pretest a module, and develop test cases. | Inspection of documented review reports and test records that include the time spent to prepare, conduct, and perform post-review or test activities (Method 1); Review of the objective evidence of the errors identified during the testing processes or traceability of safety requirements to the tests completed. If objective evidence is not available, the |

| Dependability Critical Characteristic | Description | Acceptance Criteria | Possible Verification Method |
|---|---|---|---|
| | | The thoroughness of computer program testing criteria can be measures that identify the quantity of errors discovered during the various testing activities and traceability of tests performed as they relate to software safety requirements. | dedicating entity may be able to create the traceability of the safety requirements to the tests performed from the computer program's documented requirements and test reports (Method 2). |
| Built-in quality: Training, knowledge, and proficiency of the personnel performing work | Staff training, knowledge, and proficiency associated with the design, development, testing, oversight of the program, experience in similar projects, and familiarity with specific tools, languages used design, and implementation. This critical characteristic can provide an indicator of the remaining errors in the program. | Staff training, knowledge, and proficiency criteria may include how well the specific staff member satisfies the supplier's qualification requirements for the position held. The criterion can be the percentage of qualification requirements met. | Review of objective evidence of attendance at courses, staff resumes, and on-the-job training as it relates to supplier qualification requirements to determine how well the staff member satisfies the requirements (Method 2). |

Nuclear Science and Engineering Division
Argonne National Laboratory
9700 South Cass Ave, Bldg 208
Argonne, IL 60439-4842

www.anl.gov

Argonne National Laboratory is a U.S. Department of Energy
laboratory managed by UChicago Argonne, LLC